明　細　書

デジタルコンテンツ配信システム

技術分野

本発明は、ネットワークを用いて、サーバ装置から映像、音楽などのデジタルコンテンツと、デジタルコンテンツの利用を許諾するライセンスを配信し、ユーザが端末装置でデジタルコンテンツを利用するシステムに関し、特に、前記サーバ装置と前記端末装置間の通信において、不正にライセンスの複製や改ざんが行われることを防ぎつつ、通信切断発生時においてもライセンスの消失や二重配信をも防ぐシステムおよび装置に関する。

背景技術

近年、音楽、映像、ゲーム等のデジタルコンテンツ（以下、コンテンツと記述）を、インターネット等の通信やデジタル放送等を通じて、サーバ装置から端末装置に配信し、端末装置においてコンテンツを利用することが可能な、コンテンツ配信システムと呼ばれるシステムが実用化段階に入っている。一般的なコンテンツ配信システムでは、コンテンツの著作権を保護し、悪意あるユーザ等によるコンテンツの不正利用を防止するため、著作権保護技術が用いられる。著作権保護技術とは、具体的には、暗号技術等を用いて、ユーザがコンテンツを再生したり、記録メディアにコピーしたりといったようなコンテンツの利用を、セキュアに制御する技術である。

例えば、特許文献１には、コンテンツ配信システムの一例として、暗号化されたコンテンツ、利用条件、および、コンテンツ復号鍵を端末装置が、サーバ装置より受信し、改ざん検出を行った後、利用条件の適合検証を行い、すべての検証を満足したときのみコンテンツの復号を行い

出力するシステムが記載されている。

このように、従来のコンテンツ配信システムでは、サーバ装置からライセンス（利用条件とコンテンツ復号鍵の総称。利用権利とも呼ぶ）を端末装置に配信するが、その配信経路は一般的にインターネットなどの公衆回線を用いるため、ライセンスの盗聴および改ざんを防ぐ必要がある。つまり、利用条件の不正改ざんやコンテンツ鍵の流出を防止しなければならない。さらに、サーバ装置はライセンス配信先の認証も行う必要がある。つまり、サーバ装置が意図しない端末装置にライセンスを配信することも防止する必要がある。盗聴・改ざん防止と通信相手の認証を行うプロトコルはＳＡＣ（Ｓｅｃｕｒｅ　Ａｕｔｈｅｎｔｉｃａｔｅｄ　Ｃｈａｎｎｅｌ）プロトコルと呼ばれ、例えば、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）がよく知られている（非特許文献１）。

また、通信装置・通信回線の故障や電源断などによる通信切断がライセンス配信中に発生した場合、そのライセンスが消失してしまう可能性がある。このような場合、購入したコンテンツを再生することができないといった不利益がユーザに発生する。例えば、特許文献２および特許文献３には、通信切断による通信データの消失を、データ再送によって回避するプロトコルが記載されている。

（特許文献１）：特許第３２７６０２１号公報

（特許文献２）：特開２００２－２５１５２４号公報

（特許文献３）：特開２００３－１６０４１号公報

（非特許文献１）：A.Frier, P.Karlton, and P.Kocher, "The SSL 3.0 Protocol", [online], NetScape Communications Corp., Nov. 18, 1996, [平成 15 年 1 月 17 日検索], インターネット<URL: http://wp.netscape.com/eng/ssl3/draft302.txt>

しかしながら、ＳＡＣプロトコルや通信切断対策プロトコルは、その

適用範囲を広げるために汎用性を重視し、それぞれ独立に提案されている。これにより、双方のプロトコルを利用することで、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するためには、双方のプロトコルで必要な通信往復回数が必要となる。

また、ライセンス取得やライセンス返却などのトランザクションを連続して行う場合、トランザクション毎にＳＡＣプロトコルと通信切断対策プロトコルを単純に繰り返すことにすれば、１回のトランザクション処理にかかる通信往復回数の倍数だけ通信往復回数が増えていくこととなる。例えば、１回のトランザクション処理にかかる通信往復回数を４回とする場合、ｎ個のトランザクションを処理する際には４ｎ回の通信往復回数が必要となる。

それゆえ、端末装置がトランザクション処理を完了するまでに通信遅延が発生し、ユーザが要求を出してから、応答を得るまでに待ち時間が発生するという課題がある。

発明の開示

本発明の目的は、こうした従来の問題点を解決するものであり、ライセンスの盗聴･改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するとともに、複数トランザクション処理を行う場合において、サーバ装置・端末装置間の通信往復回数を減少させ、さらに、上記機能を実現するためにサーバ装置と端末装置で管理・保持する情報が少ないプロトコルを実現するシステムおよび装置を提供することである。これにより、ユーザが要求を出してから、応答を得るまでの待ち時間を短縮させることが可能なコンテンツ配信システムを提供することを目的としている。

上記目的を達成する端末装置は、要求メッセージの送信、応答メッ

セージの受信、１つのトランザクション完了を確定させるためのコミットメッセージの送信を含むトランザクション処理に基づいてサーバ装置からコンテンツの利用に対するライセンスを取得し、前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置であって、現在のトランザクション処理について処理中であるか処理済みであるかを示す１ビットのトランザクション識別フラグを保持する保持手段と、連続する複数回のトランザクション処理における最終回を除く各トランザクション処理においてコミットメッセージを送信しないで、２回目以降の要求メッセージの送信時に、コミットメッセージの代わりに前記トランザクション識別ビットを送信する送信手段とを備える。

また、上記目的を達成するサーバ装置は、要求メッセージの受信、応答メッセージの送信、１つのトランザクション完了を確定させるためのコミットメッセージの受信を含むトランザクション処理に基づいて端末装置にコンテンツの利用に対するライセンスを提供するサーバ装置であって、連続する複数回のトランザクション処理における２回目以降の要求メッセージと共に前記コミットメッセージの代わりに送信される１ビットのフラグであって、端末装置においてトランザクションを処理中であるか処理済みであるかを示すトランザクション識別フラグを受信する受信手段と、受信されたトランザクション識別フラグに基づいて１つのトランザクションの完了を確定するか否かを判定する判定手段とを備える。

この構成によれば、端末装置とサーバ装置とを含むコンテンツ配信システムで複数トランザクション処理を行う場合、要求メッセージと同時にコミットメッセージの代用としてトランザクション識別フラグを送信する。つまり、従来別々に送信される前後する２つトランザクション処理のコミットメッセージと要求メッセージとを、上記構成では１つのメ

ッセージに重ねて送信している。このように、コミットメッセージを送信しないのでサーバ装置と端末装置との間のメッセージ往復回数を減少させることができる。さらに、サーバ装置および端末装置で１ビットのトランザクション識別フラグという少ない情報量で、メッセージ往復回数の削減と同時に通信切断対策を同時に行うことができる。これにより、ユーザがコンテンツ利用要求を出してから、応答を得るまでの待ち時間を短縮させることができる。

ここで、前記端末装置は、前記複数のトランザクション処理においてサーバ装置から送信される各応答メッセージを受信する応答受信手段と、応答受信手段による受信結果に従って、前記保持手段に保持されたトランザクション識別フラグを更新する更新手段とを備える構成としてもよい。また、前記更新手段は、前記サーバ装置に保持されるトランザクション識別フラグと同じ値を、保持手段に保持されるトランザクション識別フラグの初期値として設定し、応答受信手段によって応答メッセージが受信されたとき、保持手段のトランザクション識別フラグの値を反転する構成としてもよい。

ここで、前記サーバ装置は、前記トランザクション識別フラグは、端末装置によってトランザクションが処理される毎に反転された値を有し、前記サーバ装置は、さらに、前記複数のトランザクション処理における前回の要求メッセージと共に送信されたトランザクション識別フラグのコピーである第１フラグを保持する保持手段を備え、前記判定手段は、受信手段によって受信された現在のトランザクション処理におけるトランザクション識別フラグと、保持手段に保持された第１フラグとが不一致であるとき、前回のトランザクションの完了を確定すると判定する構成としてもよい。

この構成によれば、サーバ装置内の判定手段は、前回のトランザクシ

ョン識別フラグのコピーである第１フラグと、受信された現在のトランザクション識別フラグとを比較することにより、端末装置において前回のトランザクション処理が完了したか否かを判定することができる。

ここで、前記端末装置は、前記トランザクション識別フラグの初期値は、前記複数のトランザクション処理においてサーバ装置から送信される初回の応答メッセージに含まれ、前記更新手段は、応答受信手段によって初回の応答メッセージが受信されたとき、保持手段のトランザクション識別フラグを初期値に設定し、応答受信手段によって応答メッセージが正常に受信されたとき、保持手段のトランザクション識別フラグの値を反転する構成としてもよい。

ここで、前記サーバ装置は、前記複数のトランザクション処理における初回の応答メッセージとともに、第１フラグの初期値を前記トランザクション識別フラグの初期値として、端末装置に送信する応答送信手段を備える構成としてもよい。

この構成によれば、サーバ装置内の判定手段は、第１フラグと、受信された現在のトランザクション識別フラグとが一致する場合は、端末装置におけるトランザクション処理の状態が変化していないので、トランザクション処理が完了していないと判定し、不一致である場合は、端末装置におけるトランザクション処理の状態が変化しているので、トランザクション処理が完了したと判定する。このように、サーバ装置は、コミットメッセージを受信しなくても、トランザクション識別フラグにより簡単に端末装置におけるトランザクション処理状態(完了したか否か)を簡単に判定することできる。

ここで、前記端末装置における要求送信手段は、前記信応答受信手段によって応答メッセージが正常に受信されなかったとき、反転されていないトランザクション識別ビットを、現在のトランザクション処理の要

求メッセージとともに再度送信するように構成してもよい。

ここで、前記応答送信手段は、判定手段によって前回のトランザクションの完了を確定しないと判定されたとき、前回のトランザクション処理の応答メッセージを再度送信する構成としてもよい。

この構成によれば、例えば、通信切断という事故により端末装置が応答メッセージを正常に受信できなかった場合に、トランザクション処理を再開することができる。さらにサーバ装置は、誤った課金を防止するなどの通信切断対策を講じることができる。

ここで、前記端末装置は、複数のトランザクション処理における初回のトランザクション処理の直前にサーバ装置との間で相互認証する処理を行い、前記端末装置は、さらに、サーバ装置が端末装置を認証するための第１認証情報を認証要求として送信手段に提供し、応答受信手段によって前記第１認証情報に対する応答として受信された、端末装置がサーバ装置を認証するため第２認証情報を検証し、検証の結果、相互認証を確定させるための確定メッセージを送信手段に提供する認証手段を備え、前記送信手段は、前記確定メッセージを、前記初回のトランザクション処理の要求メッセージと共に送信する構成としてもよい。また、前記サーバ装置は、前記複数のトランザクション処理中の初回のトランザクション処理の直前にと端末装置との間で相互認証する処理を行い、前記サーバ装置は、さらに、受信手段によって認証要求として受信された、サーバ装置が端末装置を認証するための第１認証情報を検証し、正当と検証されたとき、端末装置がサーバ装置を認証するため第２認証情報を提供する認証手段を備え、前記要求受信手段は、前記初回の要求メッセージと共に、相互認証を確定させるための確定メッセージを受信するように構成してもよい。

この構成によれば、サーバ装置および端末装置は、上記認証により確

立されたセキュアな通信路を介して複数のトランザクション処理を行うので、上記の通信切断対策に加えて、正規な端末装置に見せかけるなりすましや、メッセージの改ざんや、メッセージの盗聴を防止することができる。

ここで、端末装置は、前記複数のトランザクション処理を相互認証がなされたセッションと同一のセッション上で行う構成としてもよい。

この構成によれば、ｎ個のトランザクション処理を行う場合に、従来は４ｎ回程度の通信往復回数を要していたところ、通信往復回数をｎ＋２回にまで低減することができる。

以上のように本発明の端末装置およびサーバ装置によれば、ライセンスの盗聴･改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するとともに、複数トランザクション処理を行う場合においても、サーバ装置・端末装置間の通信往復回数を減少させることができる。さらに、上記機能を実現するためにサーバ装置と端末装置で管理・保持する情報が少ないプロトコルを実現することができる。これにより、ユーザが要求を出してから、応答を得るまでの待ち時間を短縮させることができる。

図面の簡単な説明

図１は、本発明の一実施形態に係るコンテンツ配信システムの構成を示すブロック図である。

図２は、本発明の一実施形態に係るコンテンツ配信装置のセキュリティ管理／通信部の詳細な構成を示すブロック図である。

図３は、本発明の一実施形態に係るユーザ端末のセキュリティ管理／通信部の詳細な構成を示すブロック図である。

図４は、本発明の一実施形態に係るコンテンツ配信システムで行われ

るコンテンツ購入に関する処理を説明するフローチャートである。

図５は、コンテンツ権利データベース１９に格納されているコンテンツに関する情報の一例を概念的に示す図である。

図６は、ユーザデータベース１８に格納されているユーザ情報の一例を概念的に示す図である。

図７は、ユーザ所有権利データベース２０に格納されているユーザが所有する権利の情報の一例を概念的に示す図である。

図８は、コンテンツデータベース２１に格納されているコンテンツ情報の一例を概念的に示す図である。

図９は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用に関する処理を説明するフローチャートである。

図１０Ａは、コンテンツ配信装置１とユーザ端末３との間で複数のトランザクション処理を行う４種類の通信フェーズを示す説明図である。

図１０Ｂは、コンテンツ配信装置１とユーザ端末３との間で複数のトランザクション処理が正常に実行される場合のトランザクション識別ビットの遷移を示す説明図である。

図１０Ｃは、コンテンツ配信装置１とユーザ端末３との間で応答メッセージが届かなかった場合のトランザクション識別ビットの遷移を示す説明図である。

図１０Ｄは、コンテンツ配信装置１とユーザ端末３との間で要求メッセージが届かなかった場合のトランザクション識別ビットの遷移を示す説明図である。

図１１は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末３とコンテンツ配信装置１との初期フェーズにて行われる処理を説明するフローチャートである。

図１２は、本発明の一実施形態に係るコンテンツ配信システムで行わ

れるコンテンツ利用処理において、ユーザ端末３とコンテンツ配信装置１との初期フェーズ後、初回コマンド通信フェーズを開始する前にユーザ端末３において行われる処理を説明するフローチャートである。

図１３は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末３とコンテンツ配信装置１との初回コマンド通信フェーズにて行われる処理を説明するフローチャートである。

図１４は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末３とコンテンツ配信装置１とのコマンド通信フェーズにて行われる処理を説明するフローチャートである。

図１５は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末３とコンテンツ配信装置１とのコミットフェーズにて行われる処理を説明するフローチャートである。

発明を実施するための最良の形態

（実施の形態１）

図１は、本発明の一実施形態に係るコンテンツ配信システムの構成を示すブロック図である。図１において、本発明の一実施形態に係るコンテンツ配信システムは、サービス提供者側であるコンテンツ配信装置１と利用者側であるユーザ端末３とが、ネットワーク等の伝送路で接続される構成である。

コンテンツ配信装置１は、コンテンツ購入処理部１１と、ユーザ登録部１２と、ユーザ権利登録部１３と、ユーザ権利作成部１４と、コンテンツ暗号化部１５と、コンテンツ管理部１６と、セキュリティ管理／通

信部１７と、ユーザデータベース１８と、コンテンツ権利データベース１９と、ユーザ所有権利データベース２０と、コンテンツデータベース２１とを備えている。また、ユーザ端末３は、ユーザ指示処理部３１と、端末情報記憶部３２と、コンテンツ蓄積部３３と、利用権利管理部３４と、利用権利データベース３５と、セキュリティ管理／通信部３６と、出力部３７とを備えている。

まず、上記コンテンツ配信システムを構成するコンテンツ配信装置１およびユーザ端末３の概要を、以下に説明する。

コンテンツ配信装置１において、コンテンツ購入処理部１１は、コンテンツ購入処理実行時に、コンテンツ権利データベース１９に格納されている各コンテンツの内容、利用条件および料金等の情報を、ユーザ端末３へ送信してユーザに提示する。また、コンテンツ購入処理部１１は、ユーザによってコンテンツが購入された場合には、ユーザ端末３からユーザ情報（ユーザＩＤ、端末ＩＤ、ユーザ名、電話番号等）を取得すると共に、必要な課金処理を行う。コンテンツ権利データベース１９には、コンテンツ（映画やＴＶ放送等の動画、書籍や印刷物等の静止画、ラジオ放送や朗読等の音声および音楽、ゲーム等）毎に、コンテンツ利用に関する１つ又は複数の情報が格納されている。

ユーザ登録部１２は、コンテンツ購入処理部１１で取得されたユーザ情報を、ユーザデータベース１８に記憶して登録する。ユーザデータベース１８には、コンテンツ購入を行ったユーザの情報が、累積的に記憶されている。

ユーザ権利登録部１３は、ユーザ登録部１２を介してコンテンツ購入処理部１１から与えられる、ユーザが購入したコンテンツに関する情報を、ユーザが所有する権利としてユーザ所有権利データベース２０に記憶して登録する。ユーザ所有権利データベース２０には、ユーザが購入

したコンテンツの利用権利が記憶されている。

ユーザ権利作成部１４は、ユーザ端末３から受けるコンテンツ利用要求に応じて、ユーザ端末３へ送信する利用権利（利用条件、コンテンツの復号鍵）を生成する。

コンテンツ暗号化部１５は、ユーザ端末３へ送信するコンテンツの暗号化を行い、コンテンツデータベース２１へ暗号化コンテンツの登録を行う。

コンテンツ管理部１６は、ユーザ端末３へ送信する暗号化コンテンツをコンテンツデータベース２１から検索し、セキュリティ管理／通信部１７へ渡す。

セキュリティ管理／通信部１７は、ユーザ端末３の認証、コンテンツ配信装置１とユーザ端末３との間の秘匿通信（盗聴・改ざんの防止と通信相手の認証を行う通信）、および通信切断対策を行う。セキュリティ管理／通信部１７の構成および通信プロトコルの詳細については後述する。

ユーザ端末３において、ユーザ指示処理部３１は、ユーザが入力する指示(コンテンツ購入要求やコンテンツ利用要求等の指示)を処理する。

端末情報記憶部３２には、上述したユーザ情報（ユーザＩＤ、端末ＩＤ、ユーザ名、電話番号等）が記憶されている。

コンテンツ蓄積部３３には、購入によって取得された暗号化コンテンツが蓄積される。

利用権利管理部３４は、コンテンツ利用要求に応答してコンテンツ配信装置１から送信されてくる利用権利を受信し、その内容に従って、対応するコンテンツの処理（暗号解読や利用条件に基づく再生等）を実行する。この利用権利は、利用権利データベース３５に格納されて管理される。

出力部３７は、例えばディスプレイ等の表示装置であって、利用権利

管理部３４が実行する処理に応じてコンテンツの出力を行う。

セキュリティ管理／通信部３６は、コンテンツ配信装置１の認証、コンテンツ配信装置１とユーザ端末３との間の秘匿通信（盗聴・改ざんの防止と通信相手の認証を行う通信）、および通信切断対策を行う。セキュリティ管理／通信部３６の構成および通信プロトコルの詳細については後述する。

次に、コンテンツ配信装置１におけるセキュリティ管理／通信部１７の構成の詳細について図２を用いて説明する。固有鍵情報記憶部２０１は、公開鍵暗号方式におけるコンテンツ配信装置１固有の公開鍵ＫＤｓが含まれるサーバ公開鍵証明書と、コンテンツ配信装置１固有の秘密鍵ＫＥｓと、認証局公開鍵証明書とを記憶する。サーバ公開鍵証明書はコンテンツ配信装置１の公開鍵ＫＤｓに認証局の署名が施されたものである。公開鍵証明書のフォーマットには、一般的なＸ．５０９証明書フォーマットを用いるものとする。公開鍵暗号方式およびＸ．５０９証明書フォーマットについては、ＩＴＵ－Ｔ文書Ｘ．５０９"Ｔｈｅ　Ｄｉｒｅｃｒｏｒｙ：Ｐｕｂｌｉｃ－ｋｅｙ　ａｎｄ　ａｔｔｒｉｂｕｔｅ　ｃｅｒｔｉｆｉｃａｔｅ　ｆｒａｍｅｗｏｒｋｓ"が詳しい。

乱数発生部２０２は、乱数の生成を行う。生成された乱数は制御部２０４へ渡される。

暗号処理部２０３は、データの暗号化、復号、署名生成、署名検証、セッション鍵生成用パラメータの生成、セッション鍵の生成を行う。データの暗号化および復号アルゴリズムにはＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）を、署名生成および署名検証アルゴリズムにはＥＣ－ＤＳＡ（Ｅｌｌｉｐｔｉｃ　Ｃｕｒｖｅ　Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ａｌｇｏｒｉｔｈｍ）を用いる。ＡＥＳについてはＮａｔｉｏｎａｌ　Ｉｎｓｔｉｔｕｔｅ　Ｓｔａｎｄ

ａｒｄ ａｎｄ Ｔｅｃｈｎｏｌｏｇｙ（ＮＩＳＴ）、ＦＩＰＳ Ｐｕｂｌｉｃａｔｉｏｎ １９７、ＥＣ－ＤＳＡについてはＩＥＥＥ １３６３Ｓｔａｎｄａｒｄが詳しい。

暗号処理部２０３は、データの暗号化／復号を行う場合には、ＡＥＳ鍵と平文／暗号化データをそれぞれ入力とし、入力されたＡＥＳ鍵で暗号化／復号したデータをそれぞれ出力する。また、署名生成／検証を行う場合には、署名対象データ／署名検証データと秘密鍵／公開鍵をそれぞれ入力とし、署名データ／検証結果をそれぞれ出力する。さらに、セッション鍵生成用パラメータの生成を行う場合には、乱数を入力とし、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎパラメータを出力する。また、セッション鍵の生成を行う場合、乱数とＤｉｆｆｉｅ－Ｈｅｌｌｍａｎパラメータを入力とし、セッション鍵を出力する。ここで、セッション鍵の生成にはＥＣ－ＤＨ（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）を用いる。ＥＣ－ＤＨのアルゴリズムは、上記のＩＥＥＥ １３６３ Ｓｔａｎｄａｒｄが詳しい。

制御部２０４は、ユーザ端末３の認証処理、ユーザ端末３と送受信するデータの暗号化／復号、改ざんのチェックを行う。さらに、制御部２０４は、トランザクションに１ビットのトランザクション識別ビットを割り当て、そのトランザクション識別ビットと通信ステップ情報を通信ログデータベース２０６に保存することにより、通信切断対策処理を行う。ここで、トランザクションとは、「利用権利の取得」や「利用権利の返却」などの処理単位を表す。

通信部２０５は、ユーザ端末３のセキュリティ管理／通信部３６と通信を行う。

次に、ユーザ端末３におけるセキュリティ管理／通信部３６の構成の詳細について図３を用いて説明する。固有鍵情報記憶部３０１は、公開

鍵暗号方式におけるユーザ端末３固有の公開鍵ＫＤｃが含まれる端末公開鍵証明書と、ユーザ端末３固有の秘密鍵ＫＥｃと、認証局公開鍵証明書を記憶する。端末公開鍵証明書はユーザ端末３の公開鍵ＫＤｃに認証局の署名が施されたものである。公開鍵証明書のフォーマットには、コンテンツ配信装置１と同様にＸ．５０９証明書フォーマットを用いる。

乱数発生部３０２は、乱数の生成を行う。生成された乱数は制御部３０４へ渡される。

暗号処理部３０３は、データの暗号化、復号、署名生成、署名検証、セッション鍵生成用パラメータの生成、セッション鍵の生成を行う。暗号処理部３０３の入出力は、コンテンツ配信装置１の暗号処理部２０３と同じである。

制御部３０４は、コンテンツ配信装置１の認証処理、コンテンツ配信装置１と送受信するデータの暗号化／復号、改ざんのチェックを行う。さらに、制御部３０４は、コンテンツ配信装置１が生成したトランザクション識別ビットと通信ステップ情報を通信ログデータベース３０６に蓄積することにより、通信切断対策処理を行う。

通信部３０５は、ユーザ端末３側のセキュリティ管理／通信部１７と通信を行う。

次に、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ配信方法を、図４～図１２を参照して具体的に説明する。

図４は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ購入に関する処理を説明するフローチャートである。図５は、コンテンツ権利データベース１９に格納されているコンテンツに関する情報の一例を概念的に示す図である。図６は、ユーザデータベース１８に格納されているユーザ情報の一例を概念的に示す図である。図７は、ユーザ所有権利データベース２０に格納されているユーザが所有す

る権利の情報の一例を概念的に示す図である。図８は、コンテンツデータベース２１に格納されているコンテンツ情報の一例を概念的に示す図である。図９は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用に関する処理を説明するフローチャートである。図１０Ａ～１０Ｃ、図１１、図１２は、本発明の一実施形態に係るコンテンツ配信システムで行われる秘匿通信と通信切断対策処理を説明するフローチャートである。

（１）コンテンツ購入処理

図４を参照して、コンテンツ配信装置１で提供されるコンテンツをユーザが購入する際に、コンテンツ配信システムで行われる処理を説明する。

ユーザ端末３では、ユーザが、コンテンツ購入に関する指示をユーザ指示処理部３１へ出力する。ユーザ指示処理部３１は、セキュリティ管理／通信部３６を介して、指示に応じたコンテンツ購入要求をコンテンツ配信装置１へ発行する（ステップＳ４１）。

コンテンツ配信装置１では、ユーザ端末３から発行されたコンテンツ購入要求が、セキュリティ管理／通信部１７を介してコンテンツ購入処理部１１で受信される。コンテンツ購入処理部１１は、コンテンツ購入要求を受信すると、コンテンツ権利データベース１９から格納されているすべてのコンテンツに関する情報を取得し、セキュリティ管理／通信部１７を介してユーザ端末３へ送信する（ステップＳ４２）。

ここで、コンテンツ権利データベース１９には、例えば図５に示すような情報が格納されている。図５において、コンテンツ名は、コンテンツの名称であり、コンテンツＩＤは、コンテンツを識別するために付される固有の番号である。利用条件は、通常使用される予め定めたデータ形式によって、コンテンツを利用できる具体的な条件を示すものである。

各コンテンツに設定される利用条件および金額は、１つであってもよいし、複数であってもよい。この例では、映画Ａというコンテンツには、再生回数による利用条件が設定されており、４００円を支払えば、映画Ａを２回観賞することができることを表している。

なお、利用条件には、上述した利用回数や利用時間以外にも、利用期間、記録媒体へのコピーや書面への印刷の可否等の様々な条件を使用することが可能である。

再び図４を参照して、ユーザ端末３において、コンテンツ購入処理部１１から送信されたコンテンツに関する情報（図５）が確認され、ユーザがいずれかのコンテンツの購入を決定した場合（ステップＳ４３，Ｙｅｓ）、ユーザ指示処理部３１は、コンテンツ購入決定通知（購入したコンテンツおよび選択した利用条件の情報を含む）と共に、端末情報記憶部３２に格納されているユーザ情報を、セキュリティ管理／通信部３６を介してコンテンツ配信装置１へ送信する（ステップＳ４４）。

コンテンツ配信装置１では、ユーザ端末３から送信されるコンテンツ購入決定通知およびユーザ情報を、セキュリティ管理／通信部１７を介してコンテンツ購入処理部１１で受信する。そして、コンテンツ購入処理部１１は、必要な課金処理を実行すると共に、購入されたコンテンツの情報とユーザ情報とを、ユーザ登録部１２へ送出する（ステップＳ４５）。なお、課金処理は本発明の主眼ではないので、説明を省略する。

ユーザ登録部１２は、コンテンツ購入処理部１１から送出される購入されたコンテンツの情報およびユーザ情報を、ユーザ権利登録部１３へ転送すると共に、ユーザ情報をユーザデータベース１８に記憶して登録する（ステップＳ４７）。このとき、コンテンツ購入処理部１１から送出されるユーザ情報と同一の内容が、既にユーザデータベース１８に登録されている場合には、上述したユーザ登録は行われない（ステップＳ４

６、Ｙｅｓ）。

ユーザデータベース１８には、例えば図６に示すような情報が格納される。図６において、ユーザＩＤは、ユーザを識別するために付される固有の番号である。ユーザ名は、ユーザの名前である。端末ＩＤは、端末を識別するために付される固有の番号であり、１人のユーザが複数の端末を所有している場合等に利用される。電話番号は、ユーザを特定するために利用される。図６の例では、"ユーザＩＤ「０００１」である「一朗」というユーザが、ＩＤ番号「１２３４５６７」の端末を利用する"という内容が、ユーザ情報として登録されている。

ユーザ権利登録部１３は、購入によってユーザが所有することになるコンテンツ利用の権利を、ユーザ登録部１２から与えられる購入されたコンテンツの情報とユーザ情報とに基づいて、ユーザ所有権利データベース２０に記憶して登録する（ステップＳ４８）。

ユーザ所有権利データベース２０には、例えば図７に示すような情報が格納されている。図７において、ユーザＩＤは、ユーザデータベース１８に登録されている情報である。コンテンツＩＤおよび利用条件は、コンテンツ権利データベース１９に登録されている情報である。

上記処理によって、コンテンツの購入およびその購入に伴うユーザの所有権利の登録が完了する。

（２）コンテンツ利用処理

次に、図９を参照して、上述した処理によってユーザ所有権利データベース２０にユーザ所有権利が登録された後、ユーザが購入したコンテンツを利用する際にコンテンツ配信システムで行われる処理を説明する。

ユーザ端末３では、ユーザが、コンテンツ利用に関する指示をユーザ指示処理部３１へ出力する。このとき、ユーザは、コンテンツをどのように利用するのかの指示を与える。例えば、購入したコンテンツの利用

条件が回数であれば何回利用したいのか、時間であれば何分利用したいのかという指示を与える。ユーザ指示処理部３１は、セキュリティ管理／通信部３６を介して、指示に応じたコンテンツ利用要求をコンテンツ配信装置１へ送信する(ステップＳ９１)。なお、コンテンツ利用要求は、必ずしもユーザ指示に従って作成されるものではなく、ユーザ端末３内で自動的に作成される場合もある。例えば、端末３がサポートするコンテンツの利用条件が固定されている場合、ユーザが指示を与えるまでもなく、コンテンツ利用要求をユーザ端末３内で作成することができる。具体的には、ユーザ端末３が、記憶容量の制限により毎回１回分の利用権利だけが取得・処理可能な端末の場合であり、この場合には端末に応じたコンテンツ利用要求をユーザ指示処理部３１で自動的に作成し、コンテンツ配信装置１へ発行する。このコンテンツ利用要求には、上記指示の内容、ユーザＩＤ、端末ＩＤおよびコンテンツＩＤが含まれる。

コンテンツ配信装置１では、ユーザ端末３から送信されたコンテンツ利用要求を、セキュリティ管理／通信部１７を介してユーザ権利作成部１４で受信する。ユーザ権利作成部１４は、コンテンツ利用要求を受信すると、この要求に対応した内容が登録されているか否かを、ユーザデータベース１８およびユーザ所有権利データベース２０を参照して確認する（ステップＳ９２)。具体的には、ユーザ権利作成部１４は、コンテンツ利用要求に含まれるユーザＩＤおよび端末ＩＤが、ユーザデータベース１８に登録されているか否かをまず確認し、登録されていると判断すると、そのユーザＩＤにおいてコンテンツ利用要求に含まれるコンテンツＩＤおよび指示に応じた利用条件が、ユーザ所有権利データベース２０に登録されているか否かを確認する。

上記ステップＳ９２における確認の結果、コンテンツ利用要求に対応した内容が登録されていると判断した場合（ステップＳ９３，Ｙｅｓ)、

ユーザ権利作成部１４は、コンテンツ利用要求に応じた利用権利を作成し、セキュリティ管理／通信部１７を介してユーザ端末３へ送信する（ステップＳ９４）。また、ユーザ権利作成部１４は、コンテンツ利用要求に含まれるコンテンツＩＤをコンテンツ管理部１６へ通知する。コンテンツ管理部１６は、コンテンツＩＤに対応するコンテンツをコンテンツデータベース２１から取り出し、セキュリティ管理／通信部１７を介してユーザ端末３へ送信する（ステップＳ９５）。

一方、上記ステップＳ９２における確認の結果、コンテンツ利用要求に対応した内容が登録されていないと判断した場合（ステップＳ９３，Ｎｏ）、ユーザ権利作成部１４は、コンテンツ利用要求を拒絶する旨を、セキュリティ管理／通信部１７を介してユーザ端末３へ通知する（ステップＳ９７）。

ここで、上記ステップＳ９４で行われる利用権利の生成は、次のようにして行われる。前提として、ユーザＩＤ「０００１」のユーザが、図７のユーザ所有権利データベース２０に示される登録内容で、事前にコンテンツの購入を行っていたと仮定する。

さらに、そのユーザが、コンテンツＩＤ「１１２２３３」のコンテンツを１回利用したいというコンテンツ利用要求を送信してきた場合を考える。この場合、ユーザ所有権利データベース２０に登録されている利用条件が２回であるので、ユーザ権利作成部１４は、要求通り再生回数＝１を与える情報および該当コンテンツの復号鍵を含む利用権利を作成する。また、ユーザ権利作成部１４は、この利用権利の作成と同時に、ユーザ所有権利データベース２０に登録されている利用条件の回数を１つ減少させて、登録内容を更新する（図７の例では、２→１）。ただし、通信切断対策処理において、セキュリティ管理／通信部１７から再開トランザクションとして指示された場合には、登録内容の更新を行わない。

なお、通信切断対策処理については後述する。

なお、ユーザ権利作成部１４は、通信切断対策処理により再開トランザクションが発行されることを想定して、作成したユーザ権利を保存しておいてもよい。これにより、再開トランザクション発行時にユーザ権利を再度作成する手間を省くことができる。

なお、ユーザ端末３へ利用権利を発行する毎に、ユーザ所有権利データベース２０に登録されている内容を更新した結果、コンテンツの購入によって与えられた利用条件がなくなった場合には、ユーザ所有権利データベース２０に登録されている該当ユーザ所有権利を削除してもよいし、そのまま残しておいてもよい。残しておく場合には、同一のユーザが再度同じコンテンツの購入を行ったときや、ユーザが取得した利用権利を行使せずに返却するとき等に、処理対応がしやすくなる。

再び図９を参照して、ユーザ端末３において、コンテンツ配信装置１から送信される暗号化コンテンツは、コンテンツ蓄積部３３に蓄積され、利用権利は、利用権利管理部３４に入力される。利用権利管理部３４は、取得した利用権利に含まれる復号鍵を用いて該当コンテンツに施された暗号を解読し、利用条件に従って暗号解読したコンテンツの再生処理等を、出力部３７を通して実行する（ステップＳ９６）。なお、取得された利用権利は、利用権利データベース３５に格納され、コンテンツの再生回数や累積時間等の管理に利用される。

上記処理によって、要求される利用条件に応じたコンテンツを配信することができる。

（３）秘匿通信・通信切断処理

まず、図１０Ａを参照して、上述したコンテンツ利用処理において、コンテンツの利用要求（図９のステップＳ９１）、および、利用権利とコンテンツの送信（図９のステップＳ９４、Ｓ９５）が複数回行われる際

に、セキュリティ管理／通信部１７、３６で行われる、認証処理、利用権利の盗聴・改ざん防止処理、および通信切断対策処理の概略を説明する。

ユーザ端末３とコンテンツ配信装置１との通信は、すべてユーザ端末３から開始されるリクエストメッセージと、前記リクエストメッセージに呼応してコンテンツ配信装置１から返信されるレスポンスメッセージからなる。リクエストとレスポンスとの対をフェーズと呼び、秘匿通信・通信切断処理は図１０に示すとおり４種類のフェーズからなる。

初期フェーズＰ１は、ユーザ端末３とコンテンツ配信装置１との間でセッションが確立された後、最初に１度だけ行われる相互認証用のフェーズである。この初期フェーズＰ１について、初期フェーズＰ１以前のトランザクションが正常に終了していた場合と、通信切断等により異常終了していた場合とに分けて初期フェーズＰ１について説明する。

以前のトランザクションが正常に終了している場合、初期フェーズＰ１においてユーザ端末３は、コンテンツ配信装置１がユーザ端末３を認証するための認証情報Ａを初回の要求メッセージとしてコンテンツ配信装置１に送信する。コンテンツ配信装置１は、認証情報Ａを検証した後、ユーザ端末３がコンテンツ配信装置１を認証するため認証情報Ｂを送信する。その際、認証情報Ｂと共に、コンテンツ配信装置１からユーザ端末３に、トランザクション識別ビットＴの初期値（例えば０）が送信される。ユーザ端末３が認証情報Ｂを検証した後、相互認証を確定させるための認証情報Ｃは、単独で送信されないで、次の初回コマンド通信フェーズＰ２における要求メッセージと共に送信される。また、以前のトランザクションが通信切断等により異常終了している場合には、正常終了していた場合の上記の処理と比べて、コンテンツ配信装置１から送信されるトランザクション識別ビットＴの値とトランザクションを再開す

る点とが異なる。すなわち、コンテンツ配信装置１は、正常に終了していないトランザクションで用いていたトランザクション識別ビットの値をそのまま（つまり反転しないで）送信する。さらにコンテンツ配信装置１は、次の要求メッセージを、異常終了した以前のトランザクションの再開トランザクションに対する要求とみなす。

初回コマンド通信フェーズＰ２は、初期フェーズＰ１に続いて１度だけ行われるフェーズである。初回コマンド通信フェーズＰ２によって、最初のトランザクションが処理される。この初回コマンド通信フェーズＰ２において、ユーザ端末３は、要求メッセージと共に、認証情報Ｃおよびトランザクション識別ビットＴを送信する。ここで送信されるトランザクション識別ビットＴの値は、前回のトランザクション処理が正常に完了した場合コンテンツ配信装置１から送信されたトランザクション識別ビットを反転した値であり、完了していない場合には前回の（中断している）トランザクションで用いた値である。コンテンツ配信装置１は、トランザクション識別ビットが反転している場合には、新たなトランザクションの開始と判断して、要求メッセージに対する応答メッセージをユーザ端末３に送信する。また、コンテンツ配信装置１は、トランザクション識別ビットが反転していない場合には、再開トランザクションと判断して、前回と同じ応答メッセージをユーザ端末３に送信する。正常に応答メッセージを受信したユーザ端末３は、連続してトランザクション処理を行わない場合には、コミットメッセージを送信することによりコミットフェーズＰ４に移行する。また、正常に応答メッセージを受信したユーザ端末３は、連続してトランザクション処理を行う場合には、コミットメッセージを送信しないで、次のコマンド通信フェーズＰ３ａにおける要求メッセージと共にトランザクション識別ビットＴを送信する。

コマンド通信フェーズ（Ｐ３ａ等）は、同一セッション内で２つ以上のトランザクションを処理する場合に発生するフェーズである。つまり、コンテンツの利用要求および利用権利とコンテンツの送信が複数回行われる場合に、コマンド通信フェーズＰ３ａが用いられる。コンテンツの利用要求および利用権利とコンテンツの送信が１度だけの場合は、コマンド通信フェーズＰ３は行われない。コマンド通信フェーズＰ３は、最初のトランザクションに続くトランザクション数だけ繰り返される。このコマンド通信フェーズＰ３ａでは、コミットメッセージは送信されず、コミットメッセージの代わりにトランザクション識別ビットＴが、次のコマンド通信フェーズ（Ｐ３ｂ）における要求メッセージと共に送信される。

コミットフェーズは、すべてのトランザクション処理が終了した後にコンテンツ配信装置１においてトランザクション処理の完了を確定させるためのフェーズである。

図１０Ｂは、図１０Ａに示した４つの通信フェーズにおいて、コンテンツ配信装置１とユーザ端末３との間で複数のトランザクション処理が通信切断なしに正常に実行される場合のトランザクション識別ビットＴの遷移を示す説明図である。

トランザクション識別ビットＴの初期値（例えばＴ＝０）は、初期フェーズＰ１のレスポンスと共にコンテンツ配信装置１からユーザ端末３に送信される。コンテンツ配信装置１およびユーザ端末３はそれぞれ初期値を保持する。このトランザクション識別ビットＴはユーザ端末３においてトランザクション処理が完了したときに反転される。

ユーザ端末３は、初期フェーズＰ１のレスポンスとして、トランザクション識別ビットＴと認証情報Ｃを受信したとき、トランザクション識別ビットＴを反転する（Ｔ＝１）。反転しているのは、特に異常している

トランザクションが存在しないからである。

次の初回コマンド通信フェーズＰ２においてユーザ端末３は、レスポンスを正常に受信したとき、トランザクション処理が完了したものとしてトランザクション識別ビットＴを反転する（Ｔ＝０）。次のコマンド通信フェーズＰ３ａにおいてユーザ端末３は、レスポンスを正常に受信したとき、トランザクション処理が完了したものとしてトランザクション識別ビットＴを反転する（Ｔ＝１）。このようにして、ユーザ端末３は、レスポンスを正常に受信した場合に、トランザクション識別ビットＴを反転する。

反転後のトランザクション識別ビットＴは、次のコマンド通信フェーズの要求メッセージと共に送信されるので、コンテンツ配信装置１に、ユーザ端末３におけるトランザクション処理が完了したことを通知することになる。

初回コマンド通信フェーズＰ２において、コンテンツ配信装置１は、要求メッセージと共に受信したトランザクション識別ビットＴ（＝１）と保持している初期値Ｔ（＝０）とを比較し、不一致であれば（受信したトランザクション識別ビット反転していれば）、以前の中断されたトランザクションにおけるユーザ端末３のトランザクション処理が完了したと判断し、さらに、受信したトランザクション識別ビットＴ（１）を保持する。これにより、コンテンツ配信装置１内に保持しているトランザクション識別ビットＴも更新される。

同様に、コマンド通信フェーズＰ３ａにおいて、コンテンツ配信装置１は、要求メッセージと共に受信したトランザクション識別ビットＴ（＝０）と保持している初期値Ｔ（＝１）とを比較し、不一致であれば（受信したトランザクション識別ビット反転していれば）、初回コマンド通信フェーズＰ２におけるユーザ端末３のトランザクション処理が完了した

と判断し、さらに、受信したトランザクション識別ビットＴ（＝０）を保持する。これにより、コンテンツ配信装置１内に保持しているトランザクション識別ビットＴも更新される。これ以降、コマンド通信フェーズが連続する場合も、同様である。

最後のコマンド通信フェーズの完了後、ユーザ端末３からコンテンツ配信装置１にコミットメッセージが送信される。これによりコミットフェーズＰ４が開始する。コンテンツ配信装置１はコミットメッセージを受信したとき、保持しているトランザクション識別ビットＴを削除する。ユーザ端末３は、コミットメッセージに対する応答メッセージを受信したとき、トランザクション識別ビットＴを削除する。このようにして、連続するトランザクション処理が１つのセッション上で行われる。

図１０Ｃは、コンテンツ配信装置１とユーザ端末３との間で複数のトランザクション処理が正常に実行されなかった場合のトランザクション識別ビットの遷移を示す説明図である。同図では、初回コマンド通信フェーズＰ２において、コンテンツ配信装置１が送信した応答メッセージを、通信切断等の理由によりユーザ端末３が正常に受信できなかった場合を示している。

ユーザ端末３は、正常に応答メッセージを受信できなかった場合、中断しているトランザクションを再開するために、再度初期フェーズから通信を再開させる。

同図の初期フェーズＰ１１の開始時点で、コンテンツ配信装置１およびユーザ端末３はそれぞれトランザクション識別ビットＴ＝１になっている。初期フェーズＰ１１において、認証情報Ａを受信したコンテンツ配信装置１は、内部にトランザクション識別ビットＴ（＝１）が保存されているので、そのトランザクション識別ビットＴ（＝１）と認証情報Ｂとをユーザ端末３に送信する。これを受信したユーザ端末３は、受信

したトランザクション識別ビットＴ（＝１）と保持しているトランザクション識別ビットＴ（＝１）とが一致していることから、中断しているトランザクションにおいて前に送信した要求メッセージがコンテンツ配信装置１に届いたけれども、その応答メッセージがユーザ端末３に届かなかったと判断する。この場合、前に送信した要求メッセージが届いているので、コンテンツ配信装置１もトランザクションが中断された状態にあると判断している。また、ユーザ端末３は、前回のトランザクションが中断しているので受信したトランザクション識別ビットを反転することなく保存する。

次の初回コマンド通信フェーズＰ１２において、ユーザ端末３は前に送信した要求メッセージと同じ内容の要求メッセージをトランザクション識別ビットＴ（＝１）と共に再度送信する。これを受信したコンテンツ配信装置１は、受信したトランザクション識別ビットＴ（＝１）と内部に保持しているトランザクション識別ビットＴ（＝１）が一致することから、中断したトランザクションの再開トランザクションであると判断する。この場合、トランザクションが未完了なので、コンテンツ配信装置１は内部に保存しているトランザクション識別ビットを反転しない。さらに、コンテンツ配信装置１は、要求メッセージに対応する応答メッセージを再度送信することになる。

これ以降のコマンド通信フェーズについては図１０Ｂと同様である。

図１０Ｄは、コンテンツ配信装置１とユーザ端末３との間でトランザクション処理が正常に実行されなかった場合のトランザクション識別ビットの遷移を示す説明図である。同図では、図１０Ｃと異なり、初回コマンド通信フェーズＰ２において、応答メッセージの前の要求メッセージをコンテンツ配信装置１が正常に受信できなかった場合を示している。

ユーザ端末３は、正常に応答メッセージを受信できなかった場合、中

断しているトランザクションを再開するために、再度初期フェーズから通信を再開させる。

同図の初期フェーズＰ１２の開始時点で、コンテンツ配信装置１およびユーザ端末３はそれぞれトランザクション識別ビットＴ＝０、Ｔ＝１になっている。初期フェーズＰ１２において、認証情報Ａを受信したコンテンツ配信装置１は、内部にトランザクション識別ビットＴ（＝０）が保存されているので、そのトランザクション識別ビットＴ（＝０）と認証情報Ｂとをユーザ端末３に送信する。これを受信したユーザ端末３は、受信したトランザクション識別ビットＴ（＝０）と保持しているトランザクション識別ビットＴ（＝１）とが不一致であることから、中断しているトランザクションにおいて前に送信した要求メッセージがコンテンツ配信装置１にまで届かなかったと判断する。この場合、前に送信した要求メッセージが届いていないので、コンテンツ配信装置１はトランザクションが中断された状態にあると判断していない。これに対してユーザ端末３はトランザクションの中断原因が要求メッセージの不達であると判断することができる。また、ユーザ端末３は、前回のトランザクションが中断しているので受信したトランザクション識別ビットを反転することなく保存する。

次の初回コマンド通信フェーズＰ１２において、ユーザ端末３は前に送信した要求メッセージと同じ内容の要求メッセージをトランザクション識別ビットＴ（＝１）と共に再度送信してもよいし、新たな要求メッセージを送信してもよい。なぜなら、ユーザ端末３は、トランザクションの中断原因が要求メッセージの不達であると判断しているからである。つまり、コンテンツ配信装置１では、どの要求メッセージに対しても新規トランザクションと扱われるからである。ユーザ端末３からの要求メッセージが再送または新規メッセージが送信されると、コンテンツ配信

装置１は、受信したトランザクション識別ビットＴ（＝１）と保持しているトランザクション識別ビットＴ（＝０）とが一致しないことから新たなトランザクションと判断し、受信したトランザクション識別ビットＴ（＝１）を保存する（反転することになる）。さらに、コンテンツ配信装置１は、要求メッセージに応じた応答メッセージを送信する。

これ以降の通信フェーズについては図１０Ｂと同様である。

次に、図１１～図１５を参照して、上述したコンテンツ利用処理において、コンテンツの利用要求（図９のステップＳ９１）、および、利用権利とコンテンツの送信（図９のステップＳ９４、Ｓ９５）が複数回行われる際の、各フェーズでの処理を説明する。

図１１は、コンテンツ利用処理におけるユーザ端末３とコンテンツ配信装置１との初期フェーズで行われる処理について記述している。図１２は、初期フェーズ後、初回コマンド通信フェーズを開始する前にユーザ端末３において行われる処理について記述している。図１３は初回コマンド通信フェーズで行われる処理について記述している。図１４はコマンド通信フェーズで行われる処理について記述している。さらに、図１５はコミットフェーズで行われる処理について記述している。

まず、図１１を参照して、ユーザ端末３とコンテンツ配信装置１との初期フェーズで行われる処理について説明する。ユーザ端末３のセキュリティ管理／通信部３６に含まれる制御部３０４は、ユーザ指示処理部３１からコンテンツ利用要求の送信を指示された場合、乱数発生部３０２で生成した乱数Ｒｃと、固有情報記憶部３０１に記憶している端末公開鍵証明書を、通信部３０５を介して、コンテンツ配信装置１へ送信する（ステップＳ１１０１）。

コンテンツ配信装置１のセキュリティ管理／通信部１７に含まれる制御部２０４は、通信部２０５を介してユーザ端末３から、乱数Ｒｃ、端

末公開鍵証明書を受信すると、まず、固有情報記憶部２０１に記憶している認証局公開鍵証明書と、前記端末公開鍵証明書とを、暗号処理部２０３に与えることにより、前記端末公開鍵証明書の署名検証を行う（ステップＳ１１０２）。

上記ステップＳ１１０２における署名検証の結果、検証失敗となった場合（ステップＳ１１０３，Ｎｏ）、制御部２０４は、要求を拒絶する旨を、通信部２０５を介してユーザ端末３へ通知する（ステップＳ１１０４）。

一方、上記ステップＳ１１０２における署名検証の結果、検証が成功した場合（ステップＳ１１０３，Ｙｅｓ）、制御部２０４は、乱数発生部２０２で乱数Ｒｓ、Ｒｓ２を生成し、暗号処理部２０３で、乱数Ｒｓ２を入力としてＤｉｆｆｉｅ－ＨｅｌｌｍａｎパラメータＤＨｓの生成を行う（ステップＳ１１０５）。

さらに、制御部２０４は、通信ログデータベース２０６を検索し、トランザクション識別ビットが保存されているかを調べる。その結果、トランザクション識別ビットが保存されていない場合（つまり前回のコミットフェーズで削除され正常に終了した場合）は、トランザクション識別ビットＴを初期値０とし、そうでない場合は、トランザクション識別ビットＴを保存されているトランザクション識別ビットの値に設定する。その後、ユーザ端末３から受信した乱数Ｒｃ、トランザクション識別ビットＴ、ステップＳ１１０５で生成したＤＨｓを連結したデータ（式１）の署名（式２）を暗号処理部２０３で生成する（ステップＳ１１０６）。ここで、トランザクション識別ビットＴは、この初期フェーズに続く初期コマンド通信フェーズで処理されるコンテンツ要求トランザクションに対応付けられたビットであり、今後、通信切断が発生した場合には、このトランザクション識別ビットＴを用いて、中断されたトランザクシ

ョンの再開が行われる。

Ｒｃ｜｜Ｔ||ＤＨｓ　　（式１）

Ｓ（ｓ，Ｒｃ｜｜Ｔ｜｜ＤＨｓ）　　（式２）

制御部２０４は、ステップＳ１１０５で生成した乱数ＲｓおよびＤｉｆｆｉｅ－ＨｅｌｌｍａｎパラメータＤＨｓと、トランザクション識別ビットＴと、固有鍵情報記憶部２０１に記憶しているサーバ公開鍵証明書と、ステップＳ１１０６で生成した署名（式２）をユーザ端末３に通信部２０５を介して送信する（ステップＳ１１０７）。

次に、図１２を参照して、初期フェーズ後、初回コマンド通信フェーズを開始する前にユーザ端末３において行われる処理について説明する。

ユーザ端末３のセキュリティ管理／通信部３６に含まれる制御部３０４は、通信部３０５を介してコンテンツ配信装置１から、乱数Ｒｓ、トランザクション識別ビットＴ、Ｄｉｆｆｉｅ－ＨｅｌｌｍａｎパラメータＤＨｓ、サーバ公開鍵証明書、および署名データを受信すると、まず、固有情報記憶部３０１に記憶している認証局公開鍵証明書と、前記サーバ公開鍵証明書とを、暗号処理部３０３に与えることにより、前記サーバ公開鍵証明書の署名検証を行う（ステップＳ１２０１）。

上記ステップＳ１２０１における署名検証の結果、検証失敗となった場合（ステップＳ１２０２，Ｎｏ）、制御部３０４は、コンテンツ利用要求を拒絶する旨を、ユーザ指示処理部３１へ通知する（ステップＳ１２０３）。

一方、上記ステップＳ１２０１における署名検証の結果、検証が成功した場合（ステップＳ１２０２，Ｙｅｓ）、制御部３０４は、ステップＳ１１０１で作成した乱数ＲｃとステップＳ１１０７でコンテンツ配信装置１から受信したトランザクション識別ビットＴ、およびＤＨｓを結合したデータ（式３）を生成し、そのデータ（式３）、ステップＳ１１０７

でコンテンツ配信装置１から受信した署名データ（式２）、およびサーバ公開鍵証明書を暗号処理部３０３に入力し、署名データ（式２）の検証を行う（ステップＳ１２０４）。

Ｒｃ｜｜Ｔ｜｜ＤＨｓ　　（式３）

上記ステップＳ１２０４における署名検証の結果、検証失敗となった場合（ステップＳ１２０５，Ｎｏ）、制御部３０４は、コンテンツ利用要求を拒絶する旨を、ユーザ指示処理部３１へ通知する（ステップＳ１２０３）。

一方、上記ステップＳ１２０４における署名検証の結果、検証が成功した場合（ステップＳ１２０５，Ｙｅｓ）、ユーザ端末３は通信相手が確かにコンテンツ配信装置１であることが分かる（通信相手の認証）。制御部３０４は、乱数発生部３０２で乱数Ｒｃ２を生成し、生成した乱数Ｒｃ２を暗号処理部３０３の入力としてＤｉｆｆｉｅ－Ｈｅｌｌｍａｎパラメータ ＤＨｃを生成する（ステップＳ１２０６）。

さらに、制御部３０４は、ステップＳ１１０７でコンテンツ配信装置１から受信したＤＨｓと、ステップＳ１２０６で生成したＲｃ２とから、暗号処理部３０３でセッション鍵ＫＳを生成する（ステップＳ１２０７）。

その後、制御部３０４は、ステップＳ１１０７でコンテンツ配信装置１から受信したトランザクション識別ビットＴを通信ログデータベース３０６に記憶する（ステップＳ１２０８）。これにより、トランザクション通信ビットＴに対応するコンテンツ利用要求トランザクションが開始され、レスポンス待ち状態であることがデータベースに保存される。

制御部３０４は、ステップＳ１１０７でコンテンツ配信装置１から受信した乱数ＲｓとステップＳ１２０６で生成したＤＨｃを連結したデータ（式４）の署名（式５）を暗号処理部３０３で生成し、ステップＳ１２０７で生成したセッション鍵ＫＳで、ステップＳ１１０８で保存した

トランザクション識別ビットを反転し、反転したトランザクション識別ビットＴとコンテンツ利用要求メッセージＭを暗号化する（ステップＳ１２０９）。コンテンツ利用要求メッセージは、少なくとも利用するコンテンツのコンテンツ識別子を含む。暗号化データにはシーケンス番号Ｓｅｑとハッシュ値ｈを付加する（式６）。ハッシュの対象データはシーケンス番号Ｓｅｑとコンテンツ利用要求メッセージＭとする。シーケンス番号は、セッションが開始されたとき、つまり、初期フェーズが開始される際に０にリセットされ、メッセージの送信および受信の度に１ずつ加算される通し番号である。

Ｒｓ｜｜ＤＨｃ　（式４）

Ｓ（ｃ，Ｒｓ｜｜ＤＨｃ）　（式５）

Ｅ（ＫＳ，Ｓｅｑ｜｜Ｔ｜｜Ｍ｜｜ｈ）　（式６）

制御部３０４は、ステップＳ１２０６で生成したＤＨｃと、ステップＳ１２０９で生成した署名（式５）と暗号化データ（式６）をコンテンツ配信装置１に通信部３０５を介して送信する（ステップＳ１２１０）。

次に、図１３を参照して、初回コマンド通信フェーズで行われる処理について説明する。

コンテンツ配信装置１のセキュリティ管理／通信部１７に含まれる制御部２０４は、通信部２０５を介してユーザ端末３から、Ｄｉｆｆｉｅ－ＨｅｌｌｍａｎパラメータＤＨｃ、署名データ、および暗号化データを受信すると、ステップＳ１１０５で作成した乱数ＲｓとステップＳ１２１０でユーザ端末３から受信したＤＨｃを結合したデータ（式７）を生成し、その生成データ（式７）、ステップＳ１２１０でユーザ端末３から受信した署名データ、および端末公開鍵証明書を暗号処理部２０３に入力し、署名データの検証を行う（ステップＳ１３０１）。

Ｒｓ｜｜ＤＨｃ　（式７）

上記ステップＳ１３０１における署名検証の結果、検証失敗となった場合（ステップＳ１３０２，Ｎｏ）、制御部２０４は、コンテンツ利用要求を拒絶する旨を、通信部２０５を介してユーザ端末３へ通知する（ステップＳ１３０３）。

一方、上記ステップＳ１３０１における署名検証の結果、検証が成功した場合（ステップＳ１３０２，Ｙｅｓ）、コンテンツ配信装置１は通信相手が確かにユーザ端末３であることが分かる（通信相手の認証）。制御部２０４は、ステップＳ１２１０でユーザ端末３から受信したＤＨｃと、ステップＳ１１０５で生成したＲｓ２とから、暗号処理部２０３でセッション鍵ＫＳを生成する。その後、ステップ１２１０で受信した暗号化データと生成したＫＳを暗号処理部２０３に入力し暗号化データの復号を行い、シーケンス番号とハッシュ値のチェックを行う（ステップＳ１３０４）。

さらに、制御部２０４は、通信ログデータベースを検索し、トランザクション識別ビットを取得する。その結果、トランザクション識別ビットが存在しない、もしくは、その値がステップＳ１２１０で受信したトランザクション識別ビットＴと一致しない場合（ステップＳ１３０５，Ｎｏ）、コンテンツ配信装置１は、要求メッセージが新規のトランザクションのものと判断し、制御部２０４は、ステップＳ１３０１でユーザ端末３から受信したトランザクション識別ビットＴを通信ログデータベース２０６に記憶する（ステップＳ１３０６）。これにより、トランザクション識別ビットＴが反転することになる。また、コンテンツ利用要求トランザクションが、このステップまで完了したことがデータベースに保存される。

その後、制御部２０４はユーザ権利生成部１４に新規トランザクションとして、ステップＳ１２１０でユーザ端末３から受信したコンテンツ

利用要求を通知する（ステップＳ１３０７）。

一方、トランザクション識別ビットが既に存在し、その値がステップＳ１２１０で受信したトランザクション識別ビットＴと一致した場合（ステップＳ１３０５，Ｙｅｓ）、制御部２０４は、通信切断などのよりトランザクションが中断されたと判断し、ユーザ権利生成部１４に再開トランザクションとして、ステップＳ１２１０でユーザ端末３から受信したコンテンツ利用要求を通知する（ステップＳ１３０８）。

制御部２０４は、シーケンス番号とユーザ権利作成部１４で作成された利用権利とそれらのハッシュ値をステップＳ１３０４で生成したセッション鍵ＫＳを用いて暗号処理部２０３で暗号化して、通信部２０５を介してユーザ端末３に送信する(ステップＳ１３０９)。ここで、送信される利用権利は、コンテンツ配信装置１とユーザ端末３のみで生成可能なセッション鍵ＫＳで暗号化されているため、第三者が盗聴することはできない。

ユーザ端末３のセキュリティ管理／通信部３６に含まれる制御部３０４は、通信部３０５を介してコンテンツ配信装置１から、暗号化データを受信すると、まず、暗号処理部３０３でセッション鍵ＫＳを用いて暗号化データの復号を行い、シーケンス番号、利用権利、ハッシュ値を復元する。その後、シーケンス番号とハッシュ値のチェックを行い、利用条件をユーザ指示処理部３１へ通知する。さらに、通信ログデータベース３０６に保存しているトランザクション識別ビットを反転させる。(ステップＳ１３１０)。これにより、トランザクション識別ビットＴに対応するトランザクションが完了したこととなる。

この後、引き続きトランザクションがある場合にはステップＳ１４０１へ、そうでない場合はステップＳ１５０１へ移る。

次に、図１４を参照して、コマンド通信フェーズで行われる処理につ

いて説明する。

制御部３０４は、初期化フェーズで生成したセッション鍵ＫＳで、通信ログデータベース３０６に記憶するトランザクション識別ビットＴとコンテンツ利用要求メッセージＭを暗号化する（ステップＳ１４０１）。コンテンツ利用要求メッセージは、少なくとも利用するコンテンツのコンテンツ識別子を含む。暗号化データにはシーケンス番号Ｓｅｑとハッシュ値ｈを付加する。ハッシュの対象データはシーケンス番号Ｓｅｑとコンテンツ利用要求メッセージＭとする。

制御部３０４は、ステップＳ１４０１で生成した暗号化データをコンテンツ配信装置１に通信部３０５を介して送信する（ステップＳ１４０２）。

コンテンツ配信装置１のセキュリティ管理／通信部１７に含まれる制御部２０４は、通信部２０５を介してユーザ端末３から暗号化データを受信すると、暗号化データと初回コマンド通信フェーズで生成した生成したＫＳを暗号処理部２０３に入力し暗号化データの復号を行い、シーケンス番号とハッシュ値のチェックを行う（ステップＳ１４０３）。

さらに、制御部２０４は、通信ログデータベースを検索し、ステップＳ１４０２でユーザ端末３から受信したトランザクション識別ビットＴと通信ログデータベースに保持するトランザクション識別ビットと一致するかを調べる。その結果、一致しない場合（ステップＳ１４０４，Ｎｏ）、制御部２０４は、ステップＳ１４０２でユーザ端末３から受信したＴに通信ログデータベース２０６の内容を変更する（ステップＳ１４０５）。これにより、トランザクション識別ビットＴが反転することになる。また、コンテンツ利用要求トランザクションが、このステップまで完了したことがデータベースに保存される。

その後、制御部２０４はユーザ権利生成部１４に新規トランザクショ

ンとして、ステップＳ１４０２でユーザ端末３から受信したコンテンツ利用要求を通知する（ステップＳ１４０６）。

一方、トランザクション識別ビットＴが通信ログデータベース２０６に保持するトランザクション識別ビットと一致する場合（ステップＳ１４０４，Ｙｅｓ）、制御部２０４は、通信切断等によりトランザクションが中断されたものと判断し、ユーザ権利生成部１４に再開トランザクションとして、ステップＳ１４０２でユーザ端末３から受信したコンテンツ利用要求を通知する（ステップＳ１４０７）。

制御部２０４は、シーケンス番号とユーザ権利作成部１４で作成された利用権利とそれらのハッシュ値を初回コマンド通信フェーズで生成したセッション鍵ＫＳを用いて暗号処理部２０３で暗号化して、通信部２０５を介してユーザ端末３に送信する(ステップＳ１４０８)。ここで、送信される利用権利は、コンテンツ配信装置１とユーザ端末３のみで生成可能なセッション鍵ＫＳで暗号化されているため、第三者が盗聴することはできない。

ユーザ端末３のセキュリティ管理／通信部３６に含まれる制御部３０４は、通信部３０５を介してコンテンツ配信装置１から、暗号化データを受信すると、まず、暗号処理部３０３でセッション鍵ＫＳを用いて暗号化データの復号を行い、シーケンス番号、利用権利、ハッシュ値を復元する。その後、シーケンス番号とハッシュ値のチェックを行い、利用条件をユーザ指示処理部３１へ通知する。さらに、通信ログデータベース３０６に保存しているトランザクション識別ビットＴを反転する。(ステップＳ１４０９)。これにより、トランザクション識別ビットＴに対応するトランザクションが完了したこととなる。

この後、引き続きトランザクションがある場合にはステップＳ１４０１へ、そうでない場合はステップＳ１５０１へ移る。

最後に、図１５を参照して、コミットフェーズで行われる処理を説明する。

制御部３０４は、初期化フェーズで生成したセッション鍵ＫＳで、コミットメッセージを暗号化する（ステップＳ１５０１）。

制御部３０４は、ステップＳ１５０１で生成した暗号化データをコンテンツ配信装置１に通信部３０５を介して送信する（ステップＳ１５０２）。

コンテンツ配信装置１のセキュリティ管理／通信部１７に含まれる制御部２０４は、通信部２０５を介してユーザ端末３から暗号化データを受信すると、暗号化データと初回コマンド通信フェーズで生成した生成したＫＳを暗号処理部２０３に入力し暗号化データの復号を行う（ステップＳ１５０３）。

さらに、制御部２０４は、通信ログデータベース２０６に記憶しているトランザクション識別ビットを削除する（ステップＳ１５０４）。

制御部２０４は、ＡＣＫメッセージを初回コマンド通信フェーズで生成したセッション鍵ＫＳを用いて暗号処理部２０３で暗号化して、通信部２０５を介してユーザ端末３に送信する(ステップＳ１５０５)。

ユーザ端末３のセキュリティ管理／通信部３６に含まれる制御部３０４は、通信部３０５を介してコンテンツ配信装置１から、暗号化データを受信すると、まず、暗号処理部３０３でセッション鍵ＫＳを用いて暗号化データの復号を行い、ＡＣＫメッセージを復元し、コミット処理が完了したことをユーザ指示処理部３１へ通知する。その後、通信ログデータベース３０６に保存しているトランザクション識別ビットＴを削除する。(ステップＳ１５０６)。

なお、通信切断後のトランザクション再開処理は、ユーザ指示処理部３１からのトランザクション再開処理要求によって開始され、初期フェ

ーズを処理した後、通信切断により中断されているトランザクションに対応するトランザクション識別ビット（通信ログデータベースに保存されているトランザクション識別ビット）Ｔを用いて、初回コマンド通信フェーズによって再開される。この初回コマンド通信フェーズで送信されるコンテンツ利用要求メッセージは、ユーザ指示処理部３１が再度、制御部３０４に渡してもよいし、制御部３０４が通信ログデータベースにトランザクション識別ビットを保存する際にコンテンツ利用要求メッセージも保存するようにし、その保存しておいたメッセージを利用してもよい。

上記処理により、ユーザ端末３の認証処理、利用権利の盗聴・改ざん防止処理、および通信切断対策処理を行うことが可能となる。

本実施の形態で示した通信プロトコルにおいて、ｎ個のトランザクションを処理する際の通信往復回数は、初期フェーズで１往復、初回コマンド通信フェーズで１往復、コマンド通信フェーズでｎ－１往復、コミットフェーズで１往復となり、合計ｎ＋２回となる。

なお、本実施の形態で用いた暗号アルゴリズム、セッション鍵共有アルゴリズム、証明書フォーマットなどは、同等の機能を持つものであれば、必ずしも記載したものを用いる必要はない。例えば、データの暗号アルゴリズムにはＴｒｉｐｌｅＤＥＳを用いてもよい。また、暗号化データに付与されるハッシュ値は、ＣＲＣなどのチェックサム値を用いてもよい。さらに、ＳＡＣプロトコルには公開鍵暗号方式の代わりに共通鍵暗号方式を用いてもよい。

なお、本実施の形態では、ユーザ端末３からの端末公開鍵証明書は、初期化フェーズ（図１１のステップＳ１１０１）において送信したが、初回コマンド通信フェーズ（図１２のステップＳ１２１０）において送信してもよい。これにより、コンテンツ配信装置１は、装置内に上記デ

一タを保持しておく必要がなくなる。この場合、コンテンツ配信装置１での端末公開鍵証明書の署名検証処理（図１１のステップＳ１１０２）は、初回コマンド通信フェーズの最初（図１３のステップＳ１３０１の直前）で行うこととなる。

なお、ステップＳ１１０７において、コンテンツ配信装置１からユーザ端末３へ送信されるデータに、ユーザ端末３から受信した乱数Ｒｃを含めてもよい。つまり、コンテンツ配信装置１から送信されるデータは、乱数Ｒｃ、乱数Ｒｓ、トランザクション識別ビットＴ、パラメータＤＨｓ、署名データとなる。これにより、ユーザ端末３は、乱数Ｒｃを端末内に保持しておく必要がなくなる。同様に、ステップＳ１２１０において、ユーザ端末３からコンテンツ配信装置１へ送信されるデータに、コンテンツ配信装置１から受信した乱数Ｒｓを含めてもよい。つまり、コンテンツ配信装置１から送信されるデータは、乱数Ｒｓ、パラメータＤＨｃ、署名データ、暗号化データとなる。

なお、本実施の形態においては、ユーザ端末３がコンテンツ配信装置１を認証する処理も含まれているが、特に必要がない場合には、認証処理を除いてもよい。

なお、本実施の形態においては、コマンド通信フェーズでトランザクション識別ビットの一致判定を行っているが、特に必要が無い場合には、判定処理を除いてもよい。この場合、コマンド通信フェーズで処理されるトランザクションは常に新規トランザクションとして処理される。

なお、本実施の形態においては、トランザクション識別ビットをコンテンツ配信装置１から送信するようにしているが、これを省略してもよい。つまり、初期フェーズにおけるコンテンツ配信装置１の処理および、初期フェーズにおけるメッセージ中のトランザクション識別ビットに関する情報は省略される。

なお、本実施の形態においては、ステップＳ１３０８およびステップＳ１４０７においてユーザ権利の作成を行う際に、セキュリティ管理／通信部１７から再開トランザクションとして指示された場合には、登録内容の更新を行わないとしたが、再度、コンテンツ利用要求を評価し、ユーザ権利の作成をやり直してもよい。これにより、新規トランザクションの発行と再開トランザクションの発行の間に起こった状況変化に対応することが可能となる。例を挙げれば、新規トランザクション発行時には、コンテンツの利用有効期限内であったので利用権利の作成・送信を行ったが、再開トランザクションとして再度要求が行われたときには、コンテンツの利用有効期限を越えたいた場合が考えられる。この場合には、再開トランザクションに対しては利用権利の作成・発行は行わない。

また、本実施の形態においては、通信切断によって処理途中のトランザクションのキャンセル処理を含めてもよい。キャンセル処理を行う場合、通信切断後の初回コマンド通信フェーズで、レスポンスをまだ受信していないトランザクションに対応するトランザクション識別ビットＴ（通信ログデータベース３０６に保存しているもの）を含むキャンセルメッセージをユーザ指示処理部３１の指示によりユーザ端末３から送信する。キャンセルメッセージを受信したコンテンツ配信装置１は、ユーザ権利作成部１４にその旨を通知し、処理途中のトランザクションを処理前の状態にロールバックさせる。その後、コンテンツ配信装置１はユーザ端末３に対して、ＡＣＫメッセージを送信する。

また、コンテンツ配信装置１とユーザ端末３との間の２つのコンテンツ利用要求処理を処理Ａおよび処理Ｂとするとき、処理Ａの終了後に、一旦、通信切断を行わなければいけない場合、通常は、処理Ｂの開始時には再度認証処理を行い、新たなセッション鍵を作成し直すが、処理Ｂの応答時間を削減したい場合には、処理Ｂでの認証処理を除くために、

処理Ａでのセッション鍵をコンテンツ配信装置１とユーザ端末３の双方で記憶しておき、再利用してもよい。

なお、本実施の形態においては、コンテンツ配信装置１はセッション鍵の利用制限を設けてもよい。例えば、セッション鍵の再利用回数が規定の上限を超えた場合、セッション鍵が最初に作成されたから規定の時間が経過した場合、セッション鍵が最初に作成されてから規定の通信データ量を超えた場合、予め決められたコンテンツあるいは利用権利を配信する場合、あるいは、予め決められたユーザ端末３に配信する場合などに、コンテンツ配信装置１はユーザ端末３にセッション鍵再利用不可通知を行う。セッション鍵再利用不可通知を受信したユーザ端末３は、セッション鍵を生成しなおす。つまり、初期フェーズから通信をやり直す。

なお、本実施の形態においては、コンテンツ配信装置１とユーザ端末３との間のプロトコルとして説明を行ったが、ユーザ端末同士でのライセンス交換にも適用可能である。例えば、家庭内のユーザ端末同士でライセンスを移動させる場合に適用できる。その際、同一家庭内のユーザ端末であるというグループ識別子が予め、あるいは、購入後の設定により指定されているものとする。ユーザ端末間でライセンスを移動させる際に本実施の形態で示したプロトコルを適用する場合、ライセンスの移動元端末をコンテンツ配信装置１に、ライセンスの移動先端末をユーザ端末３と捉えればよい。なお、ライセンスの移動を同一家庭内、つまり、同一グループ識別子を持つもの同士に限る場合には、ライセンス配信先端末からライセンス配信元端末にグループ識別子を送信し、ライセンス配信元端末が同一グループ識別子かどうかを判定し、同一である場合のみライセンスの送信を行うようにする。グループ識別子の送信は、盗聴・改ざん・成りすましを防ぐ方法であれば、どのような方法であってもよ

い。例えば、初回コマンド通信フェーズの暗号化データに含めてもよい。また、グループ識別子そのものを送信せず、グループ識別子のハッシュ値を用いてもよい。さらに、別途、グループ識別子ハッシュ送信フェーズを初期フェーズの後に設けて、セッション鍵で暗号化したグループ識別子ハッシュを送信してもよい。

なお、本実施の形態で示したコンテンツ配信システムの各構成要素は、ハードウェアで実現しても、ソフトウェアで実現してもよい。

以上のように本発明によれば、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するとともに、複数トランザクション処理を行う場合においても、サーバ装置・端末装置間の通信往復回数を減少させ、さらに、上記機能を実現するためにサーバ装置と端末装置で管理・保持する情報が少ないプロトコルを実現するシステムおよび装置を提供する。これにより、ユーザが要求を出してから、応答を得るまでの待ち時間を短縮させることが可能なコンテンツ配信システムを提供することができる。

産業上の利用可能性

本発明は、要求メッセージの受信、応答メッセージの送信、トランザクション完了を確定させるためのコミットメッセージの受信を含むトランザクション処理に基づいて端末装置にコンテンツの利用に対するライセンスを提供するサーバ装置と、前記サーバ装置から取得した前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置とを含むデジタルコンテンツ配信システムに適している。例えば、サーバ装置としては、インターネットを介してデジタルコンテンツを配信するサービスプロバイダの配信サーバや、放送を介してデジタルコンテンツをデジタル放送する放送装置等に適しており、端末装置としては、デジタル放送

を受信するためのセットトップボックス、デジタルＴＶ、ＤＶＤレコーダ、ハードディスクレコーダ、パーソナルコンピュータなどのコンテンツ再生装置、記録装置あるいはこれらの複合機器等に適している。

請　求　の　範　囲

１．要求メッセージの送信、応答メッセージの受信、１つのトランザクション完了を確定させるためのコミットメッセージの送信を含むトランザクション処理に基づいてサーバ装置からコンテンツの利用に対するライセンスを取得し、前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置であって、

現在のトランザクション処理について処理中であるか処理済みであるかを示す１ビットのトランザクション識別フラグを保持する保持手段と、

連続する複数回のトランザクション処理における最終回を除く各トランザクション処理においてコミットメッセージを送信しないで、２回目以降の要求メッセージの送信時に、コミットメッセージの代わりに前記トランザクション識別ビットを送信する送信手段と

を備えることを特徴とする端末装置。

２．前記端末装置は、

前記複数のトランザクション処理においてサーバ装置から送信される各応答メッセージを受信する応答受信手段と、

応答受信手段による受信結果に従って、前記保持手段に保持されたトランザクション識別フラグを更新する更新手段と

を備えることを特徴とする請求の範囲第１項に記載の端末装置。

３．前記更新手段は、

前記サーバ装置に保持されるトランザクション識別フラグと同じ値を、保持手段に保持されるトランザクション識別フラグの初期値として設定し、

応答受信手段によって応答メッセージが受信されたとき、保持手段の

トランザクション識別フラグの値を反転する

ことを特徴とする請求の範囲第２項に記載の端末装置。

４．前記トランザクション識別フラグの初期値は、前記複数のトランザクション処理においてサーバ装置から送信される初回の応答メッセージに含まれ、

前記更新手段は、

応答受信手段によって初回の応答メッセージが受信されたとき、保持手段のトランザクション識別フラグを初期値に設定し、

応答受信手段によって応答メッセージが正常に受信されたとき、保持手段のトランザクション識別フラグの値を反転する

ことを特徴とする請求の範囲第３項に記載の端末装置。

５．前記送信手段は、

前記複数のトランザクション処理において、２回目以降の要求メッセージの送信時に、コミットメッセージ送信の代用として前記トランザクション識別ビットを送信する要求送信手段と、

前記複数トランザクション処理中の最後のトランザクション処理においてのみコミットメッセージを送信するコミット送信手段と

を備えることを特徴とする請求の範囲第３項に記載の端末装置。

６．前記要求送信手段は、

前記信応答受信手段によって応答メッセージが正常に受信されたとき、更新手段により反転されたトランザクション識別ビットを、次のトランザクション処理の要求メッセージとともに送信する

ことを特徴とする請求の範囲第５項に記載の端末装置。

7．前記要求送信手段は、

前記信応答受信手段によって応答メッセージが正常に受信されなかったとき、反転されていないトランザクション識別ビットを、現在のトランザクション処理の要求メッセージとともに再度送信する

ことを特徴とする請求の範囲第６項に記載の端末装置。

8．前記端末装置は、複数のトランザクション処理における初回のトランザクション処理の直前にサーバ装置との間で相互認証する処理を行い、

前記端末装置は、さらに、

サーバ装置が端末装置を認証するための第１認証情報を認証要求として送信手段に提供し、

応答受信手段によって前記第１認証情報に対する応答として受信された、端末装置がサーバ装置を認証するため第２認証情報を検証し、

検証の結果、相互認証を確定させるための確定メッセージを送信手段に提供する認証手段を備え、

前記送信手段は、前記確定メッセージを、前記初回のトランザクション処理の要求メッセージと共に送信する

ことを特徴とする請求の範囲第２項に記載の端末装置。

9．前記複数のトランザクション処理を相互認証がなされたセッションと同一のセッション上で行う

ことを特徴とする請求の範囲第８項に記載の端末装置。

１０．前記更新手段は、

前記サーバ装置に保持されるトランザクション識別フラグと同じ値を、

保持手段に保持されるトランザクション識別フラグの初期値として設定し、

応答受信手段によって応答メッセージが受信されたとき、保持手段のトランザクション識別フラグの値を反転する

ことを特徴とする請求の範囲第８項に記載の端末装置。

１１．前記送信手段は、

前記複数のトランザクション処理において、２回目以降の要求メッセージの送信時に、コミットメッセージ送信の代用として前記トランザクション識別ビットを送信する要求送信手段と、

前記複数トランザクション処理中の最後のトランザクション処理においてのみコミットメッセージを送信するコミット送信手段と

を備えることを特徴とする請求の範囲第１０項に記載の端末装置。

１２．前記要求送信手段は、

前記信応答受信手段によって応答メッセージが正常に受信されたとき、更新手段により反転されたトランザクション識別ビットを、次のトランザクション処理の要求メッセージとともに送信する

ことを特徴とする請求の範囲第１１項に記載の端末装置。

１３．前記要求送信手段は、

前記信応答受信手段によって応答メッセージが正常に受信されなかったとき、反転されていないトランザクション識別ビットを、現在のトランザクション処理の要求メッセージとともに再度送信する

ことを特徴とする請求の範囲第１２項に記載の端末装置。

１４．要求メッセージの受信、応答メッセージの送信、１つのトランザクション完了を確定させるためのコミットメッセージの受信を含むトランザクション処理に基づいて端末装置にコンテンツの利用に対するライセンスを提供するサーバ装置であって、

連続する複数回のトランザクション処理における２回目以降の要求メッセージと共に前記コミットメッセージの代わりに送信される１ビットのフラグであって、端末装置においてトランザクションを処理中であるか処理済みであるかを示すトランザクション識別フラグを受信する受信手段と、

受信されたトランザクション識別フラグに基づいて１つのトランザクションの完了を確定するか否かを判定する判定手段と

を備えることを特徴とするサーバ装置。

１５．前記トランザクション識別フラグは、端末装置によってトランザクションが処理される毎に反転された値を有し、

前記サーバ装置は、さらに、

前記複数のトランザクション処理における前回の要求メッセージと共に送信されたトランザクション識別フラグのコピーである第１フラグを保持する保持手段を備え、

前記判定手段は、

受信手段によって受信された現在のトランザクション処理におけるトランザクション識別フラグと、保持手段に保持された第１フラグとが不一致であるとき、前回のトランザクションの完了を確定すると判定することを特徴とする請求の範囲第１４項に記載のサーバ装置。

１６．前記サーバ装置は、前記複数のトランザクション処理における初

回の応答メッセージとともに、第１フラグの初期値を前記トランザクション識別フラグの初期値として、端末装置に送信する応答送信手段を備える

ことを特徴とする請求の範囲第１５項に記載のサーバ装置。

１７．前記受信手段は、

前記２回目以降の要求メッセージと共に前記トランザクション識別フラグを受信する要求受信手段と、

前記複数トランザクション処理中の最後のトランザクション処理においてのみコミットメッセージを受信するコミット受信手段と

を備えることを特徴とする請求の範囲第１５項に記載のサーバ装置。

１８．前記応答送信手段は、

判定手段によって前回のトランザクションの完了を確定すると判定されたとき、次のトランザクション処理の応答メッセージを送信する

ことを特徴とする請求の範囲第１７項に記載のサーバ装置。

１９．前記応答送信手段は、

判定手段によって前回のトランザクションの完了を確定しないと判定されたとき、前回のトランザクション処理の応答メッセージを再度送信する

ことを特徴とする請求の範囲第１８項に記載のサーバ装置。

２０．前記サーバ装置は、前記複数のトランザクション処理中の初回のトランザクション処理の直前に端末装置との間で相互認証する処理を行い、

前記サーバ装置は、さらに、

受信手段によって認証要求として受信された、サーバ装置が端末装置を認証するための第１認証情報を検証し、

正当と検証されたとき、端末装置がサーバ装置を認証するため第２認証情報を提供する認証手段を備え、

前記要求受信手段は、前記初回の要求メッセージと共に、相互認証を確定させるための確定メッセージを受信する

ことを特徴とする請求の範囲第１５項に記載のサーバ装置。

２１．前記複数のトランザクション処理を相互認証がなされたセッションと同一のセッション上で行う

ことを特徴とする請求の範囲第２０項に記載のサーバ装置。

２２．前記受信手段は、

前記２回目以降の要求メッセージと共に前記トランザクション識別フラグを受信する要求受信手段と、

前記複数トランザクション処理中の最後のトランザクション処理においてのみコミットメッセージを受信するコミット受信手段と

を備えることを特徴とする請求の範囲第２１項に記載のサーバ装置。

２３．前記応答送信手段は、

判定手段によって前回のトランザクションの完了を確定すると判定されたとき、次のトランザクション処理の応答メッセージを送信する

ことを特徴とする請求の範囲第２２項に記載のサーバ装置。

２４．前記応答送信手段は、

判定手段によって前回のトランザクションの完了を確定しないと判定されたとき、前回のトランザクション処理の応答メッセージを再度送信する

ことを特徴とする請求の範囲第２３項に記載のサーバ装置。

２５．要求メッセージの受信、応答メッセージの送信、トランザクション完了を確定させるためのコミットメッセージの受信を含むトランザクション処理に基づいて端末装置にコンテンツの利用に対するライセンスを提供するサーバ装置と、前記サーバ装置から取得した前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置とを含むデジタルコンテンツ配信システムであって、

前記端末装置は、

現在のトランザクション処理について処理中であるか処理済みであるかを示す１ビットのトランザクション識別フラグを保持する保持手段と、

連続する複数回のトランザクション処理における最終回を除く各トランザクション処理においてコミットメッセージの送信を送信しないで、２回目以降の要求メッセージの送信時に、コミットメッセージの代わりに前記トランザクション識別ビットを送信する送信手段とを備え、

前記サーバ装置は、

連続する複数回のトランザクション処理における２回目以降の要求メッセージと共に送信される前記トランザクション識別フラグを受信する受信手段と、

受信されたトランザクション識別フラグに基づいて１つのトランザクションの完了を確定するか否かを判定する判定手段とを備える

ことを特徴とするコンテンツ配信システム。

２６．要求メッセージの送信、応答メッセージの受信、１つのトランザクション完了を確定させるためのコミットメッセージの送信を含むトランザクション処理に基づいてサーバ装置からコンテンツの利用に対するライセンスを取得し、前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置におけるトランザクション処理方法であって、

連続する複数回のトランザクション処理における最終回を除く各トランザクション処理においてコミットメッセージを送信しないで、２回目以降の要求メッセージの送信時に、コミットメッセージの代わりに、現在のトランザクション処理について処理中であるか処理済みであるかを示す１ビットの前記トランザクション識別ビットを送信するよう制御する制御ステップと、

前記最終回のトランザクション処理においてコミットメッセージの送信する送信ステップと

を有することを特徴とするトランザクション処理方法。

２７．要求メッセージの受信、応答メッセージの送信、１つのトランザクション完了を確定させるためのコミットメッセージの受信を含むトランザクション処理に基づいて端末装置にコンテンツの利用に対するライセンスを提供するサーバ装置におけるトランザクション処理方法であって、

連続する複数回のトランザクション処理における２回目以降の要求メッセージと共に前記コミットメッセージの代わりに送信される１ビットのフラグであって、端末装置においてトランザクションを処理中であるか処理済みであるかを示すトランザクション識別フラグを受信するステップと、

受信されたトランザクション識別フラグに基づいて１つのトランザク

ションの完了を確定するか否かを判定する判定ステップと

を有することを特徴とするトランザクション処理方法。

２８．要求メッセージの受信、応答メッセージの送信、トランザクション完了を確定させるためのコミットメッセージの受信を含むトランザクション処理に基づいて端末装置にコンテンツの利用に対するライセンスを提供するサーバ装置と、前記サーバ装置から取得した前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置とを含むデジタルコンテンツ配信システムにおけるトランザクション処理方法であって、

前記端末装置において、連続する複数回のトランザクション処理における最終回を除く各トランザクション処理においてコミットメッセージを送信しないで、２回目以降の要求メッセージの送信時に、コミットメッセージの代わりに、現在のトランザクション処理について処理中であるか処理済みであるかを示す１ビットの前記トランザクション識別ビットを送信するよう制御する制御ステップと、

前記端末装置において、前記最終回のトランザクション処理においてコミットメッセージの送信する送信ステップと

前記サーバ装置において、連続する複数回のトランザクション処理における２回目以降の要求メッセージと共に前記コミットメッセージの代わりに送信される１ビットのフラグであって、端末装置においてトランザクションを処理中であるか処理済みであるかを示すトランザクション識別フラグを受信するステップと、

前記サーバ装置において、受信されたトランザクション識別フラグに基づいて１つのトランザクションの完了を確定するか否かを判定する判定ステップと

を有することを特徴とするトランザクション処理方法。

２９．要求メッセージの送信、応答メッセージの受信、１つのトランザクション完了を確定させるためのコミットメッセージの送信を含むトランザクション処理に基づいてサーバ装置からコンテンツの利用に対するライセンスを取得し、前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置においてトランザクション処理を実行させるプログラムであって、

現在のトランザクション処理について処理中であるか処理済みであるかを示す１ビットのトランザクション識別フラグを保持する保持手段と、

連続する複数回のトランザクション処理における最終回を除く各トランザクション処理においてコミットメッセージを送信しないで、２回目以降の要求メッセージの送信時に、コミットメッセージの代わりに前記トランザクション識別ビットを送信する送信手段と

を端末装置内のコンピュータに実現させるプログラム。

３０．要求メッセージの受信、応答メッセージの送信、１つのトランザクション完了を確定させるためのコミットメッセージの受信を含むトランザクション処理に基づいて端末装置にコンテンツの利用に対するライセンスを提供するサーバ装置においてトランザクション処理を実行させるプログラムであって、

連続する複数回のトランザクション処理における２回目以降の要求メッセージと共に前記コミットメッセージの代わりに送信される１ビットのフラグであって、端末装置においてトランザクションを処理中であるか処理済みであるかを示すトランザクション識別フラグを受信する受信手段と、

受信されたトランザクション識別フラグに基づいて１つのトランザク

ションの完了を確定するか否かを判定する判定手段と

をサーバ装置内のコンピュータに実現させるプログラム。

要　約　書

本発明のコンテンツ配信システムは、要求メッセージの受信、応答メッセージの送信、トランザクション完了を確定させるためのコミットメッセージの受信を含むトランザクション処理に基づいて端末装置にコンテンツの利用に対するライセンスを提供するサーバ装置と、前記サーバ装置から取得した前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置とを含み、前記端末装置は、現在のトランザクション処理について処理中であるか処理済みであるかを示す１ビットのトランザクション識別フラグを保持する保持手段と、連続する複数回のトランザクション処理における最終回を除く各トランザクション処理においてコミットメッセージを送信しないで、２回目以降の要求メッセージの送信時に、省略されたコミットメッセージの代わりに前記トランザクション識別ビットを送信する送信手段とを備え、前記サーバ装置は、連続する複数回のトランザクション処理における２回目以降の要求メッセージと共に送信される前記トランザクション識別フラグを受信する受信手段と、受信されたトランザクション識別フラグに基づいて１つのトランザクションの完了を確定するか否かを判定する判定手段とを備える。

図1

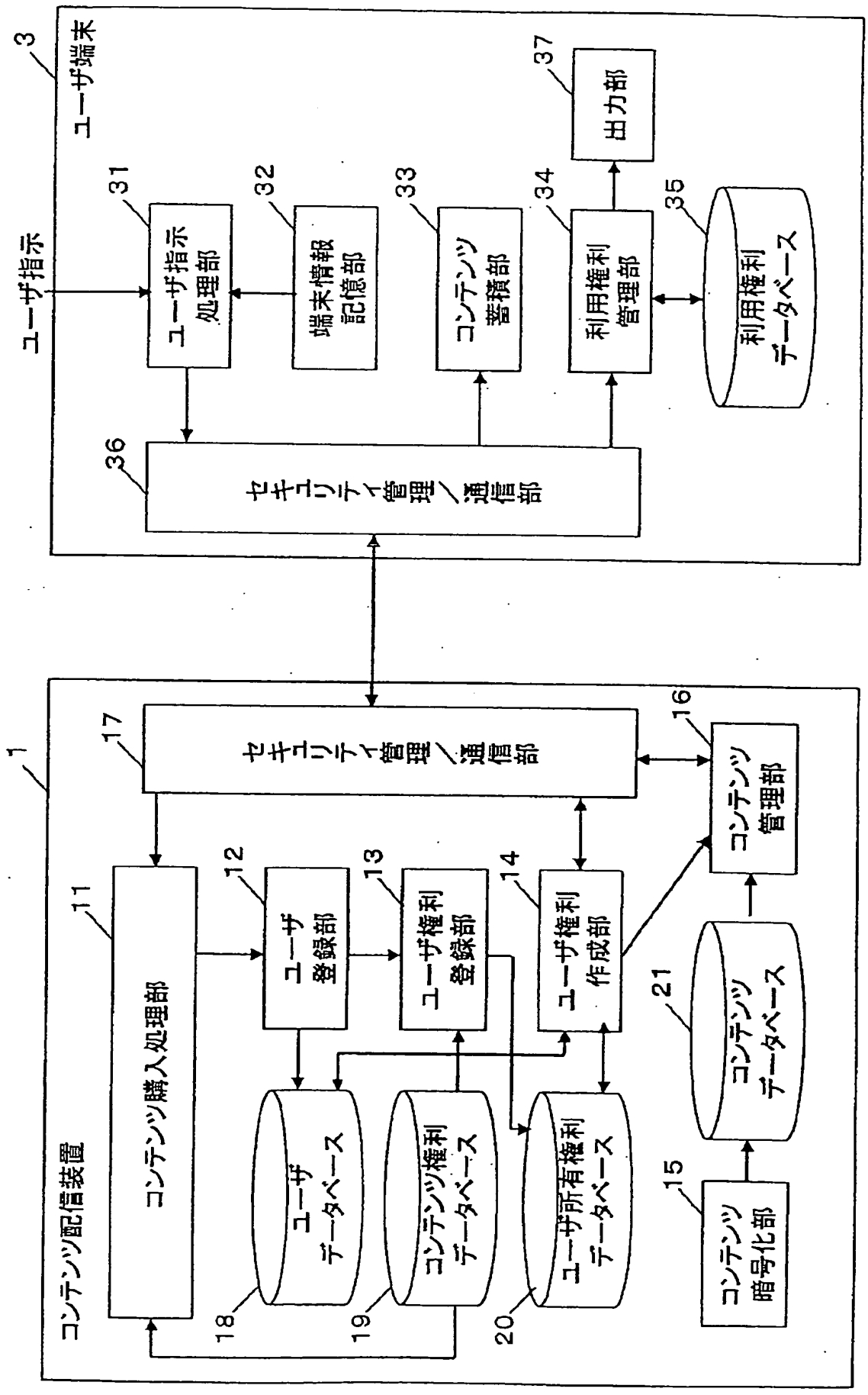

3
ユーザ端末
ユーザ指示
31
ユーザ指示処理部
32
端末情報記憶部
33
コンテンツ蓄積部
34
利用権利管理部
35
利用権利データベース
37
出力部
36
セキュリティ管理／通信部
1
コンテンツ配信装置
17
セキュリティ管理／通信部
16
コンテンツ管理部
11
コンテンツ購入処理部
12
ユーザ登録部
13
ユーザ権利登録部
14
ユーザ権利作成部
21
コンテンツデータベース
15
コンテンツ暗号化部
18
ユーザデータベース
19
コンテンツ権利データベース
20
ユーザ所有権利データベース

図2

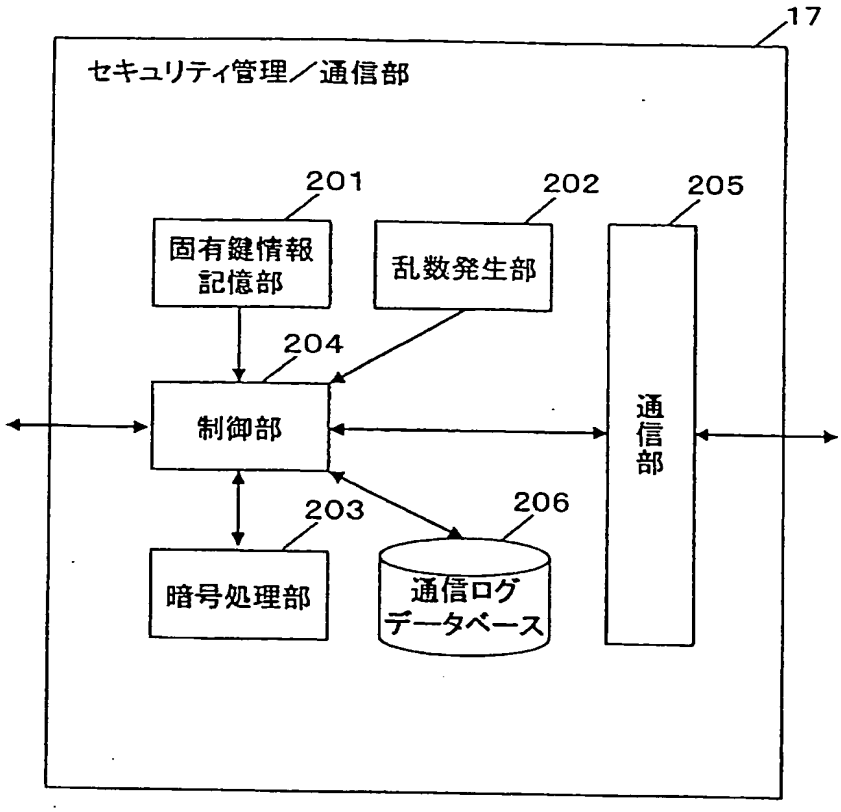

17
セキュリティ管理／通信部
201
固有鍵情報記憶部
202
乱数発生部
205
通信部
204
制御部
203
暗号処理部
206
通信ログデータベース

図3

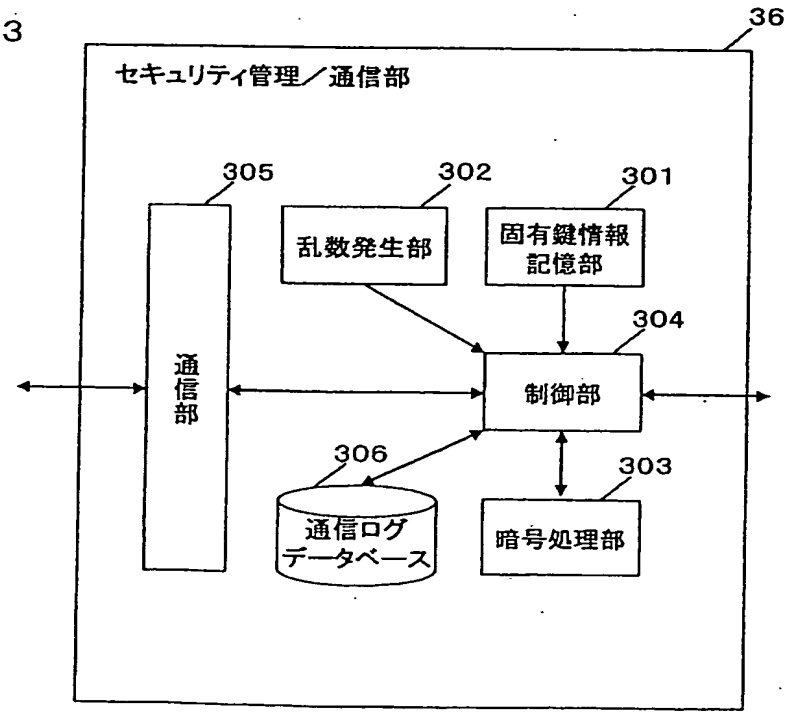

36
セキュリティ管理／通信部
305
通信部
302
乱数発生部
301
固有鍵情報記憶部
304
制御部
306
通信ログデータベース
303
暗号処理部

図4

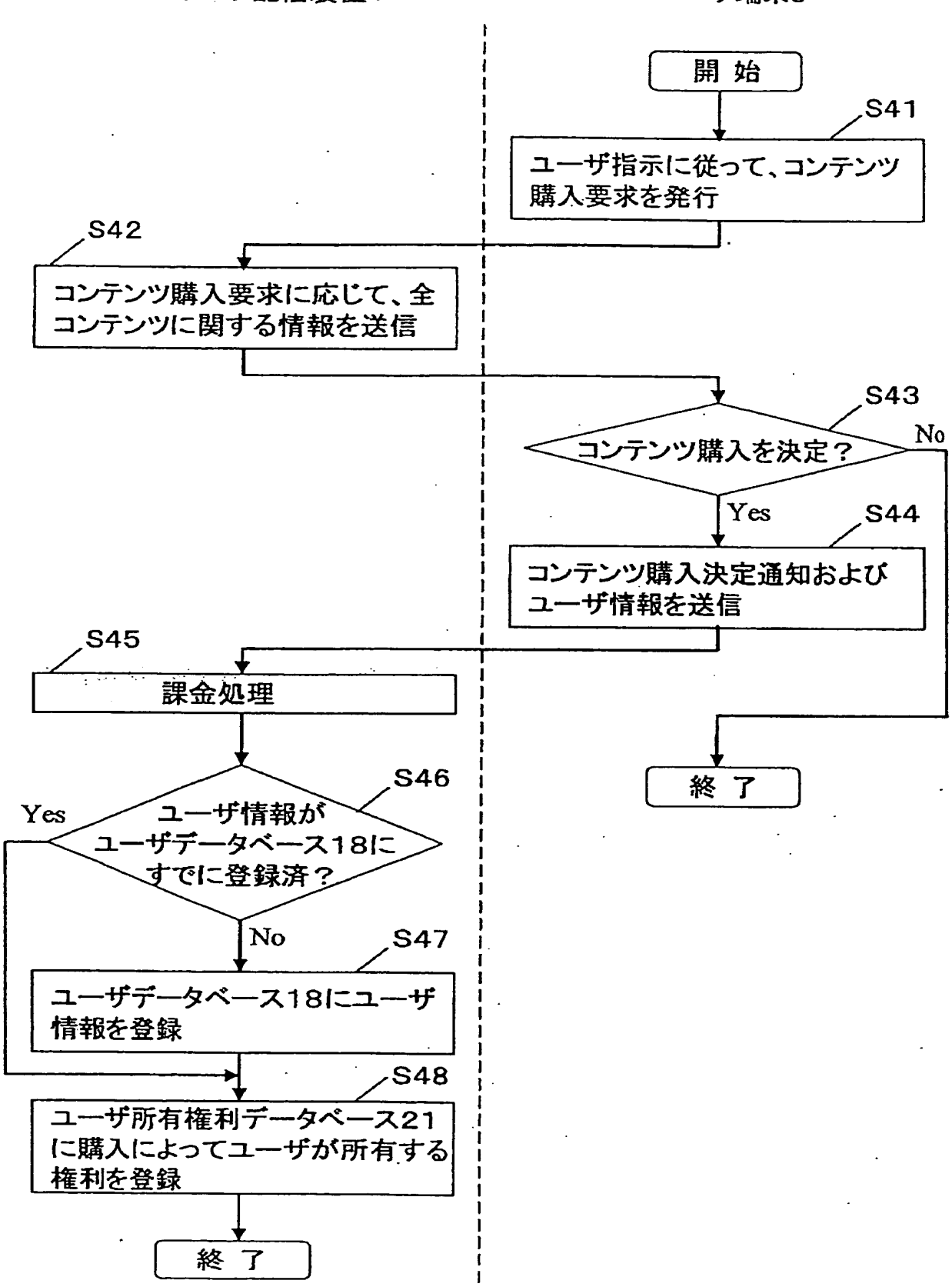

コンテンツ配信装置1
ユーザ端末3
開 始
S41
ユーザ指示に従って、コンテンツ購入要求を発行
S42
コンテンツ購入要求に応じて、全コンテンツに関する情報を送信
S43
コンテンツ購入を決定？
No
Yes
S44
コンテンツ購入決定通知およびユーザ情報を送信
S45
課金処理
S46
ユーザ情報がユーザデータベース18にすでに登録済？
Yes
No
S47
ユーザデータベース18にユーザ情報を登録
S48
ユーザ所有権利データベース21に購入によってユーザが所有する権利を登録
終 了
終 了

図5

コンテンツ名	コンテンツID	利用条件	料金
映画A	112233	再生回数＝2	400円
音楽B	334567	再生回数＝5 累積再生時間＝1H	500円 1000円
ゲームC	321098	累積再生時間＝2H 無制限	700円 2000円

図6

ユーザID	コンテンツID	利用条件
0001	112233	再生回数＝2
0002	321098	累積再生時間＝2H

図7

ユーザID	コンテンツID	利用条件
0001	112233	再生回数＝2
0002	321098	累積再生時間＝2H

図8

コンテンツID	コンテンツ名	コンテンツ暗号鍵	ファイル名
112233	映画A	0123456789..	movieA.mpg
234567	音楽B	7361278168..	musicB.wav

図9

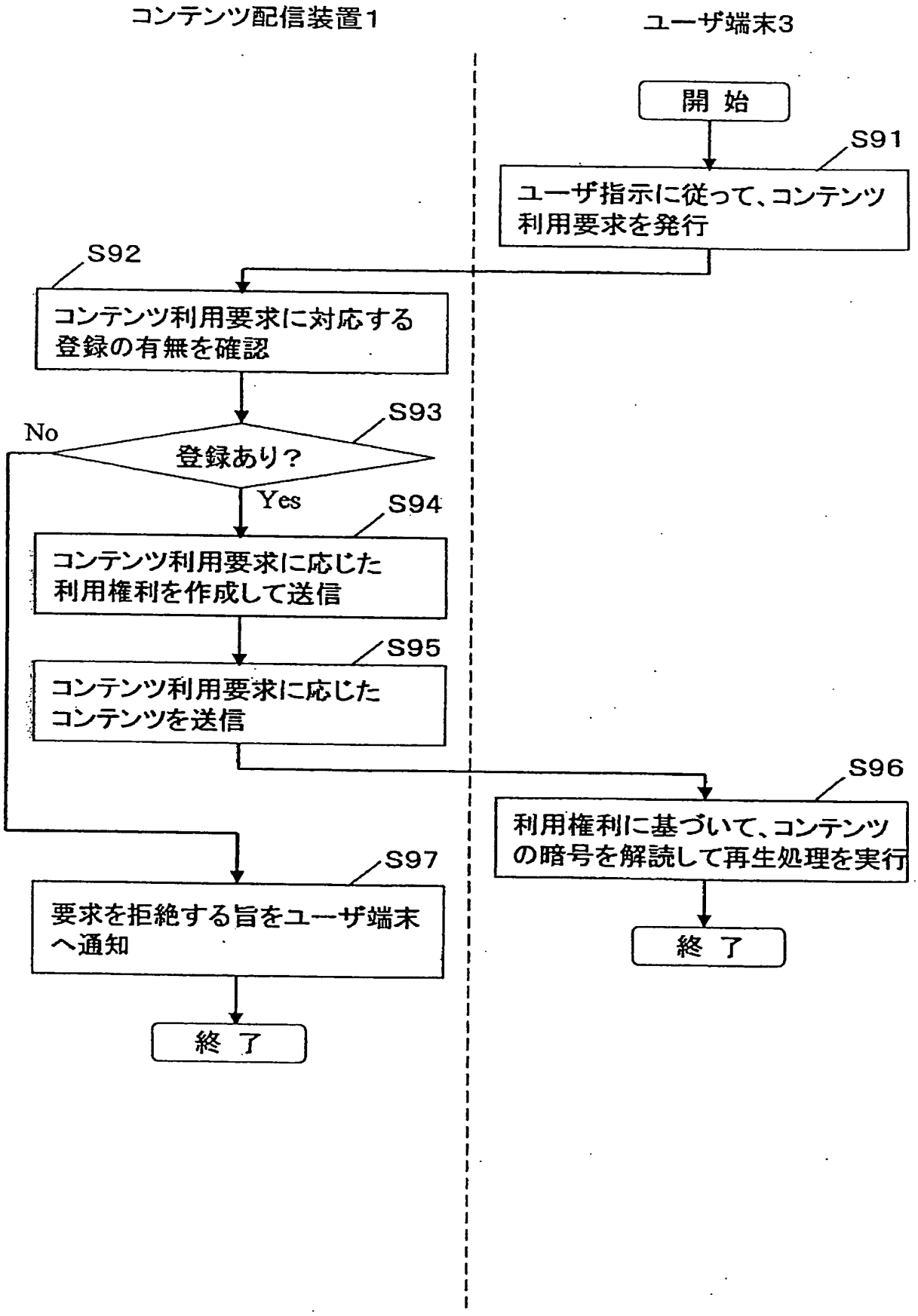

コンテンツ配信装置1
ユーザ端末3
開 始
S91
ユーザ指示に従って、コンテンツ利用要求を発行
S92
コンテンツ利用要求に対応する登録の有無を確認
S93
No
登録あり？
Yes
S94
コンテンツ利用要求に応じた利用権利を作成して送信
S95
コンテンツ利用要求に応じたコンテンツを送信
S96
利用権利に基づいて、コンテンツの暗号を解読して再生処理を実行
終 了
S97
要求を拒絶する旨をユーザ端末へ通知
終 了

図10A

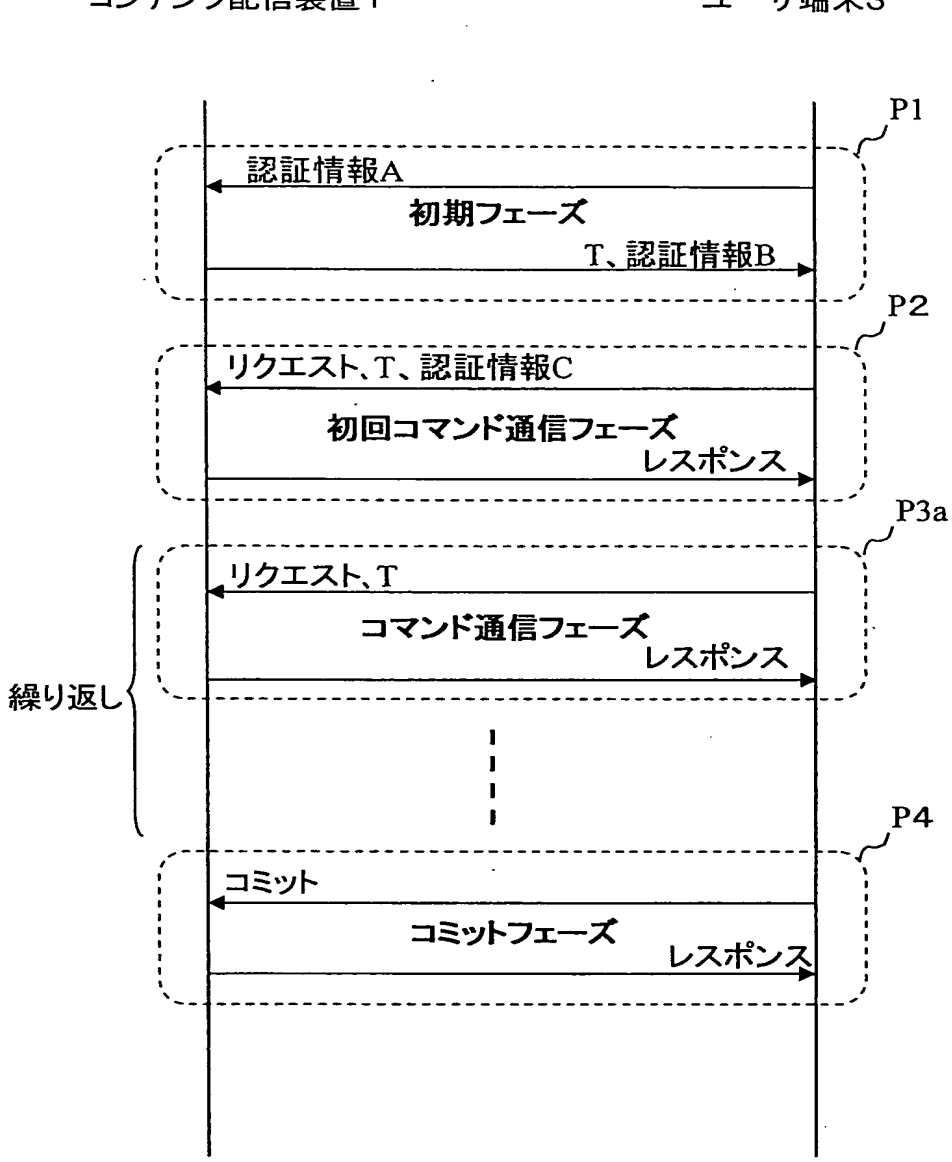

コンテンツ配信装置1
ユーザ端末3
P1
認証情報A
初期フェーズ
T、認証情報B
P2
リクエスト、T、認証情報C
初回コマンド通信フェーズ
レスポンス
P3a
リクエスト、T
コマンド通信フェーズ
レスポンス
繰り返し
P4
コミット
コミットフェーズ
レスポンス

図10B

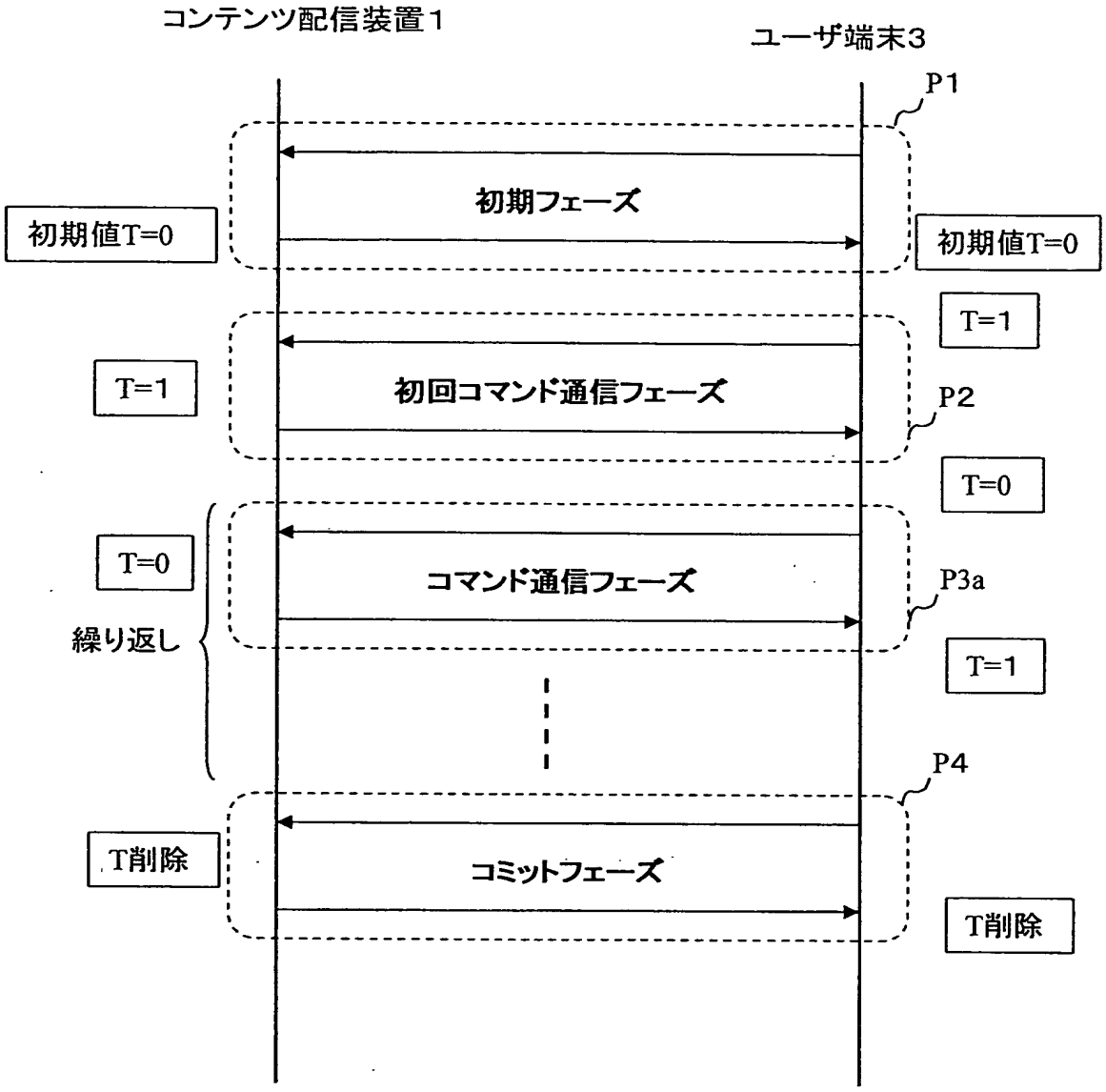

コンテンツ配信装置1
ユーザ端末3
P1
初期フェーズ
初期値T=0
初期値T=0
T=1
T=1
初回コマンド通信フェーズ
P2
T=0
T=0
コマンド通信フェーズ
P3a
繰り返し
T=1
P4
T削除
コミットフェーズ
T削除

図10C

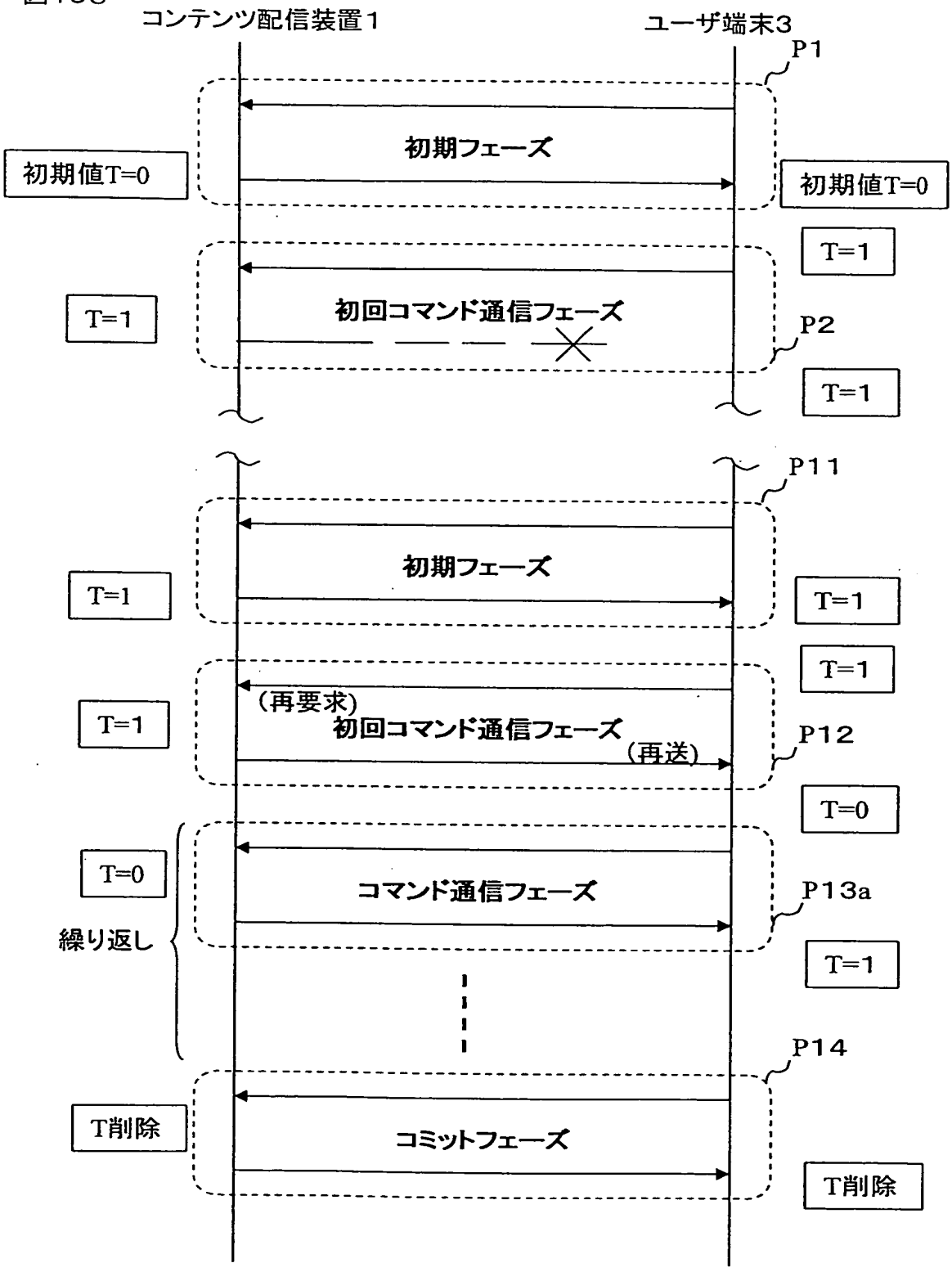

コンテンツ配信装置1
ユーザ端末3
P1
初期フェーズ
初期値T=0
初期値T=0
T=1
T=1
初回コマンド通信フェーズ
P2
T=1
P11
初期フェーズ
T=1
T=1
T=1
(再要求)
T=1
初回コマンド通信フェーズ
(再送)
P12
T=0
T=0
コマンド通信フェーズ
P13a
繰り返し
T=1
P14
T削除
コミットフェーズ
T削除

図10D

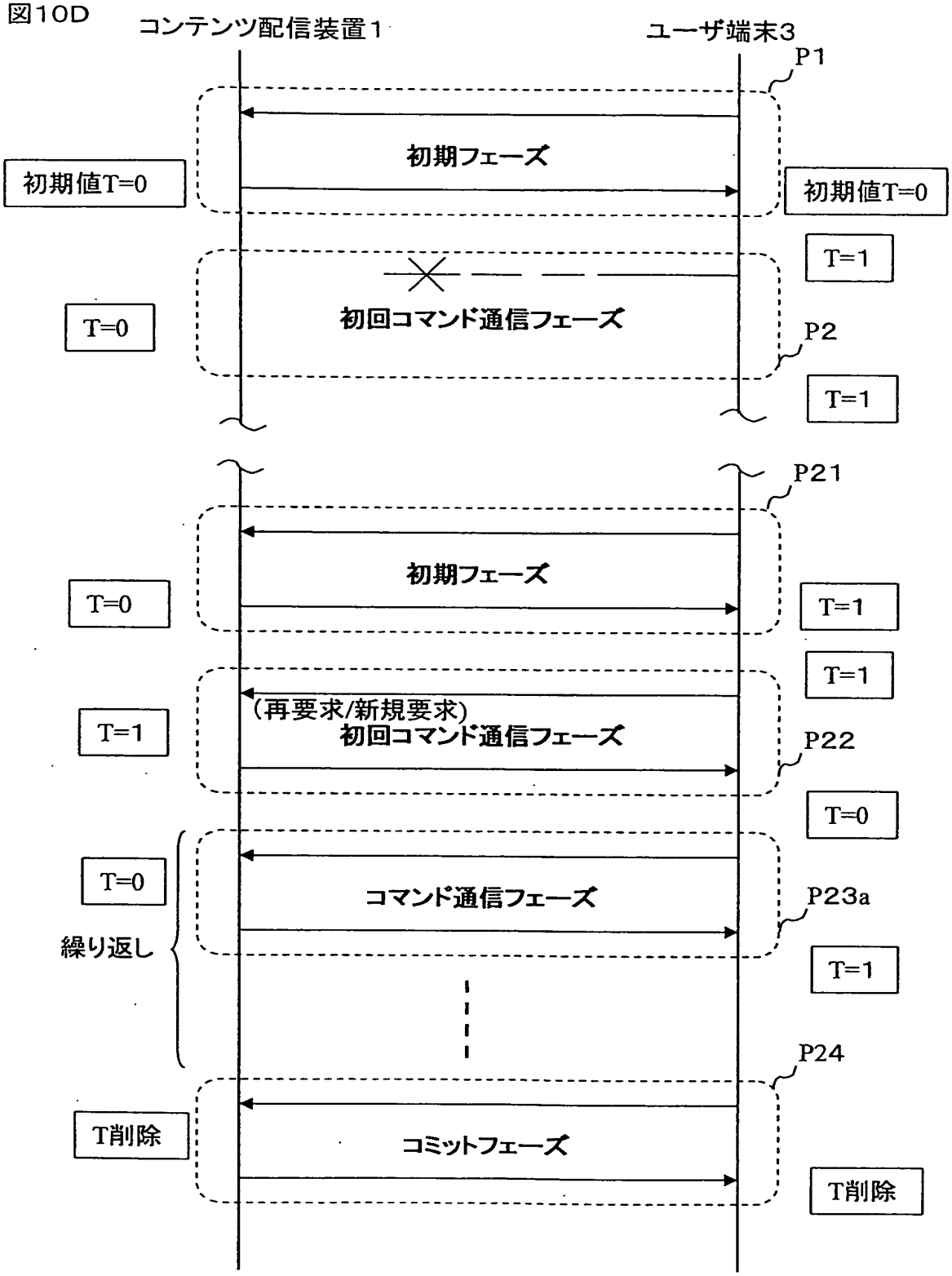

コンテンツ配信装置1
ユーザ端末3
P1
初期フェーズ
初期値T=0
初期値T=0
T=1
T=0
初回コマンド通信フェーズ
P2
T=1
P21
初期フェーズ
T=0
T=1
T=1
(再要求/新規要求)
初回コマンド通信フェーズ
T=1
P22
T=0
T=0
コマンド通信フェーズ
P23a
繰り返し
T=1
P24
T削除
コミットフェーズ
T削除

図11

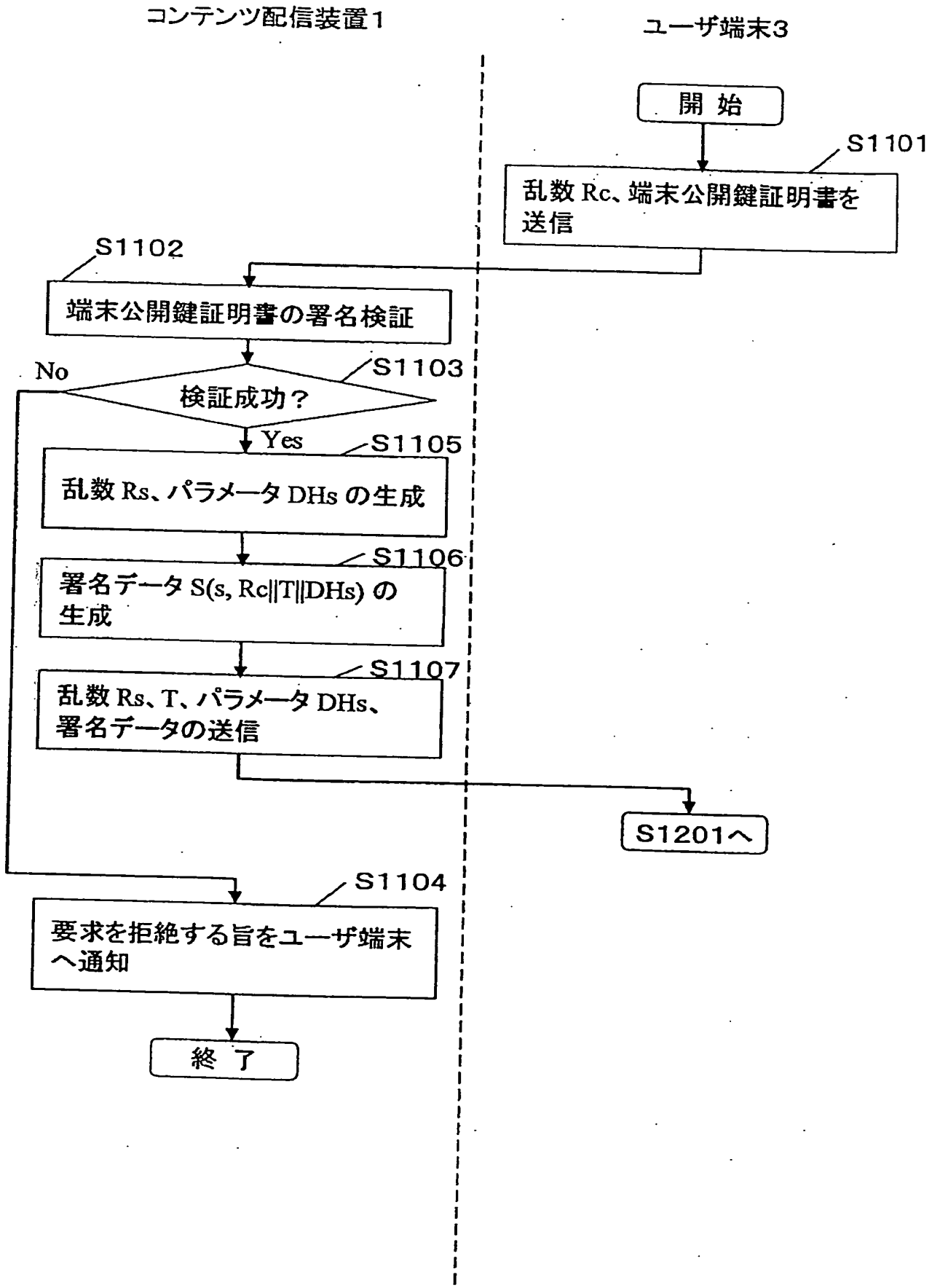

コンテンツ配信装置1
ユーザ端末3
開 始
S1101
乱数 Rc、端末公開鍵証明書を送信
S1102
端末公開鍵証明書の署名検証
No
検証成功？
S1103
Yes
S1105
乱数 Rs、パラメータ DHs の生成
S1106
署名データ S(s, Rc||T||DHs) の生成
S1107
乱数 Rs、T、パラメータ DHs、署名データの送信
S1201へ
S1104
要求を拒絶する旨をユーザ端末へ通知
終 了

図12

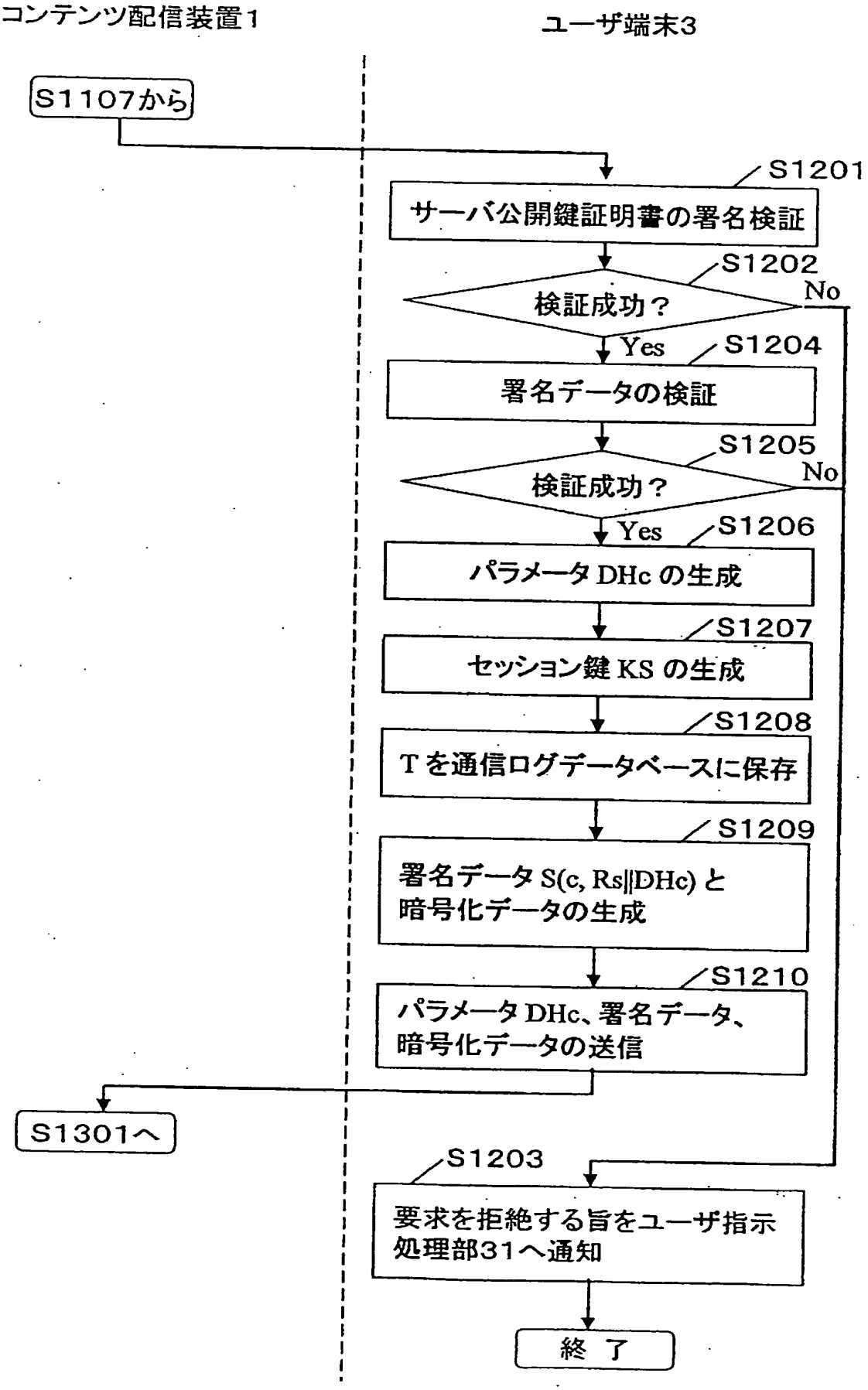

コンテンツ配信装置1
ユーザ端末3
S1107から
S1201
サーバ公開鍵証明書の署名検証
S1202
検証成功？
No
Yes
S1204
署名データの検証
S1205
検証成功？
No
Yes
S1206
パラメータ DHc の生成
S1207
セッション鍵 KS の生成
S1208
T を通信ログデータベースに保存
S1209
署名データ S(c, Rs||DHc) と
暗号化データの生成
S1210
パラメータ DHc、署名データ、
暗号化データの送信
S1301へ
S1203
要求を拒絶する旨をユーザ指示
処理部31へ通知
終 了

図13

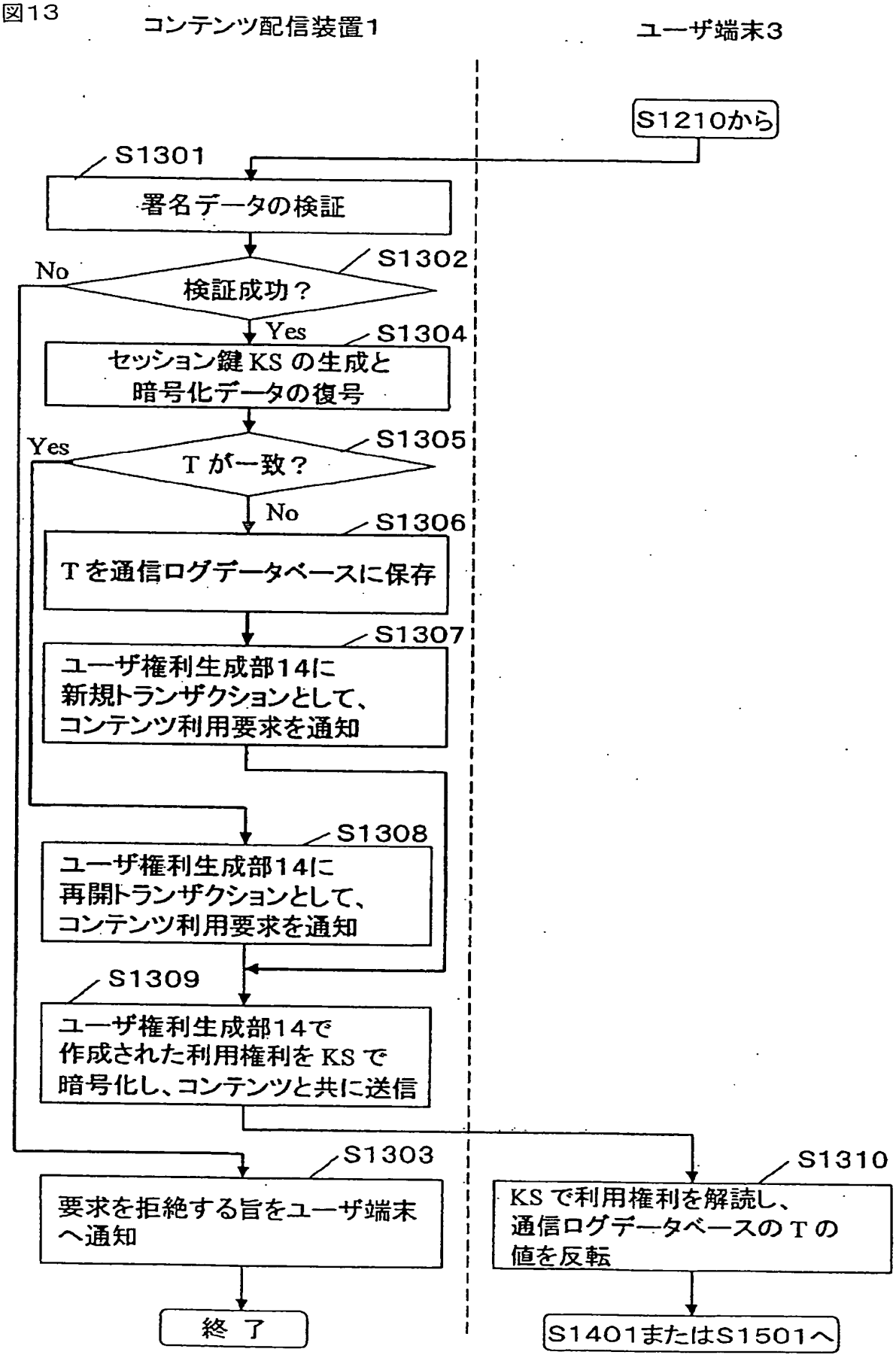

コンテンツ配信装置1
ユーザ端末3
S1210から
S1301
署名データの検証
S1302
No
検証成功？
Yes
S1304
セッション鍵KSの生成と
暗号化データの復号
S1305
Yes
Tが一致？
No
S1306
Tを通信ログデータベースに保存
S1307
ユーザ権利生成部14に
新規トランザクションとして、
コンテンツ利用要求を通知
S1308
ユーザ権利生成部14に
再開トランザクションとして、
コンテンツ利用要求を通知
S1309
ユーザ権利生成部14で
作成された利用権利をKSで
暗号化し、コンテンツと共に送信
S1303
要求を拒絶する旨をユーザ端末
へ通知
終了
S1310
KSで利用権利を解読し、
通信ログデータベースのTの
値を反転
S1401またはS1501へ

図14

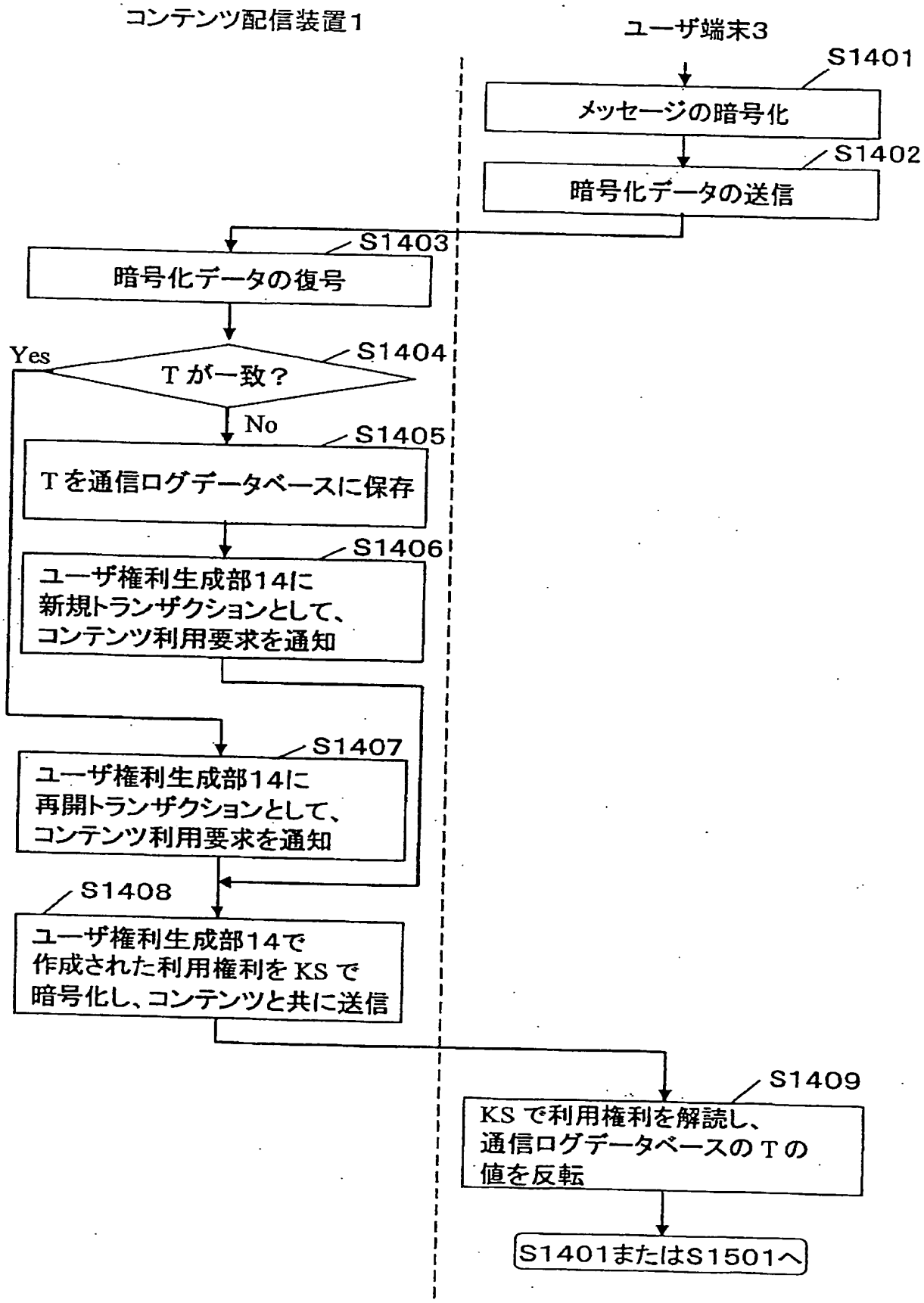
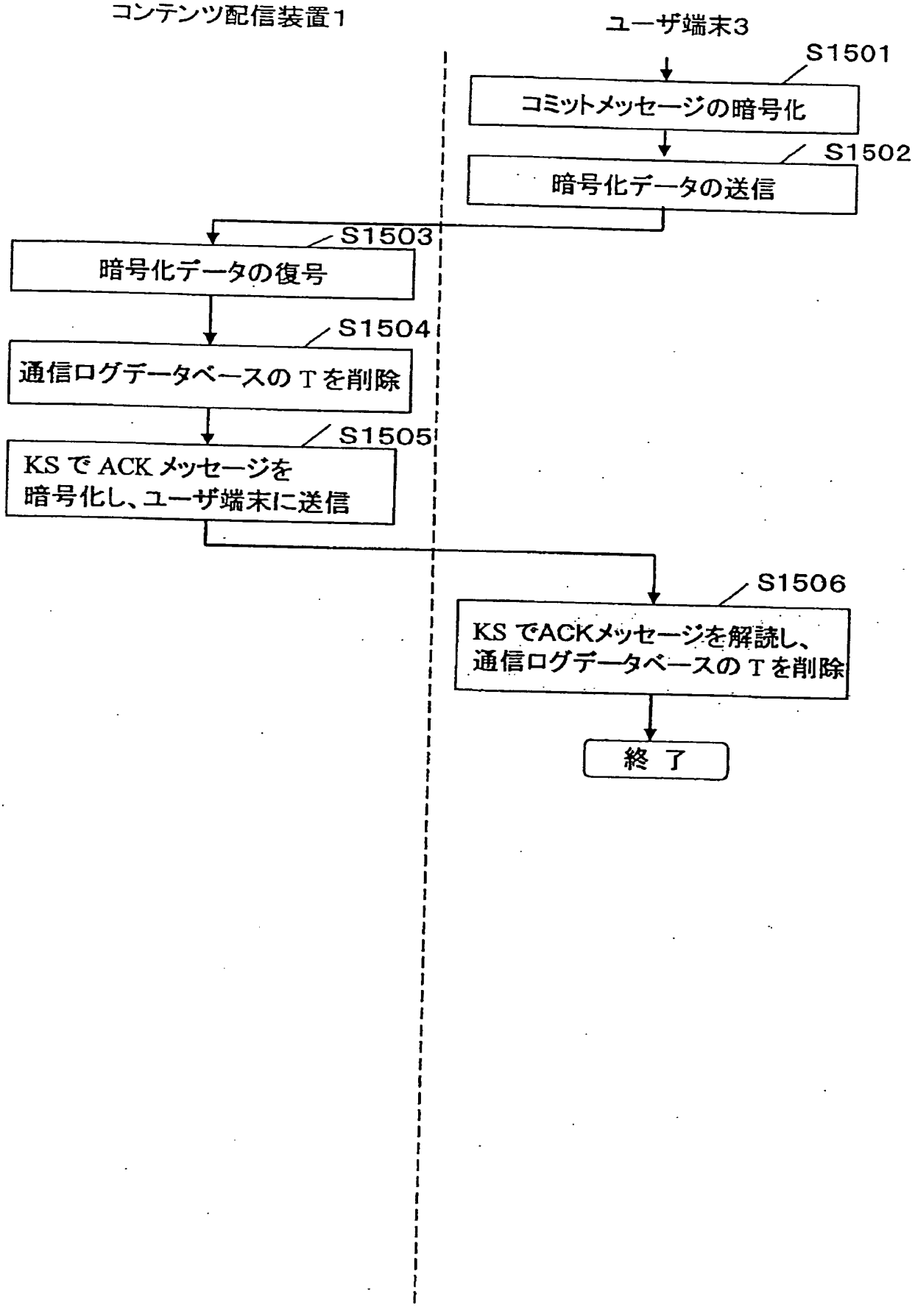

コンテンツ配信装置1
ユーザ端末3
S1401
メッセージの暗号化
S1402
暗号化データの送信
S1403
暗号化データの復号
Yes
S1404
Tが一致？
No
S1405
Tを通信ログデータベースに保存
S1406
ユーザ権利生成部14に
新規トランザクションとして、
コンテンツ利用要求を通知
S1407
ユーザ権利生成部14に
再開トランザクションとして、
コンテンツ利用要求を通知
S1408
ユーザ権利生成部14で
作成された利用権利をKSで
暗号化し、コンテンツと共に送信
S1409
KSで利用権利を解読し、
通信ログデータベースのTの
値を反転
S1401またはS1501へ

図15


コンテンツ配信装置1
ユーザ端末3
S1501
コミットメッセージの暗号化
S1502
暗号化データの送信
S1503
暗号化データの復号
S1504
通信ログデータベースのTを削除
S1505
KSでACKメッセージを
暗号化し、ユーザ端末に送信
S1506
KSでACKメッセージを解読し、
通信ログデータベースのTを削除
終了